SANS | GIAC CERTIFICATIONS

Cybersecurity Training & Certifications

Live Online and OnDemand

Plus:

- Degree Programs
- Cyber Ranges
- Free Summits
- Workshops & Resources

35+ GIAC Certifications

70+ Hands-on Courses

New! Stay Sharp Series

> "SANS is the best information security training you'll find anywhere. World-class instructors, hands-on instruction, actionable information you can really use, and NetWars."
>
> — Jeff Stebelton, **NetJets, Inc.**

sans.org | giac.org

A Letter to Our Community

The Art of the Pivot

Pivoting became one of the most crucial skills in 2020. You did it all year to meet the challenges you faced, and you have seen SANS do it several times as we navigate the continuously evolving conditions of the pandemic.

In the face of all the changes and uncertainties the past year presented, we worked tirelessly to keep our promise to you: **You will be able to apply SANS training the day you return to work.** In person or online, the quality and practicality of our training is always steady, thanks to the dedicated efforts of our course instructors, authors, and staff. And thanks to you who have been willing to adapt and to pivot with us.

For those who are hesitant to try our online training, we understand. The change from in-person to online is another layer of uncertainty topping off this period of unprecedented change. We want to reassure you that our online training options will provide you with the high-quality, relevant training you expect from SANS. Please read what our students have shared about their experiences, and consider options that will work for you.

Explore the following pages in this catalog to learn more about your online training options, and keep striving toward your goal. We will be there every step of the way to help you get there.

Sincerely,
Eric Bassel, CEO

Highlights of additional pivots SANS has made so you continue to train with industry experts, practice your skills, get certified, and connect with the community:

Free Cyber Ranges & Capture-the-Flag events

To encourage you to continue practicing and honing your skills, our Cyber Range team has offered numerous free challenges.

GIAC Certifications

Now offering remotely proctored exams or in-person testing, so you can test the way that fits your needs, from wherever you are.

Bachelor's Program

SANS Technical Institute is now offering an online Bachelor's degree program, in addition to the certificate and Master's degree program.

Free Resources

New tools, posters, blogs, podcasts, and more have been produced to support awareness and growth across a wide range of cybersecurity interests.

Free Summits

To give you more opportunities to engage with the community and learn about new topics, many of our virtual Summits will be free in 2021.

Stay Sharp Events

Offering short courses designed to equip you with cybersecurity training with less time away from home and work responsibilities.

New Courses & Major Updates

SANS course authors are developing the most up-to-date and relevant content available.

Tech Tuesday & SANS@Mic

Continually learn and expand your knowledge base with our free SANS@Mic talks and hands-on Tech Tuesday Workshops.

Live Online

What Students say about **SANS Live Online** training

"I honestly can't imagine how much effort you all put into creating and delivering this training. I was worried about the Live Online format, but I think it might actually be better than most in-person training."

—Chantel Strickland, **Cisco**

"The entire SANS Live Online package – Slack, GoToTraining, VMs, tools, etc. – are woven together to make this as close to live training as possible, and I have been able to remain engaged throughout the day."

—Andrea Doherty, **Dell Technologies**

OnDemand

What Students say about **SANS OnDemand** training

"The OnDemand delivery platform allows me to complete the course at my own pace. It works smoothly and gives me everything I need to follow the course."

—Eric Brosa, **Nestlé**

"I love the SANS OnDemand option for learning. I can tackle the material at my own pace with a blend of learning approaches (MP3s, indexing, labs, and videos when needed to highlight a challenging area). I really appreciate the quizzes at the end of each section, too."

—Andy Piazza, **phia, LLC**

Table of Contents

> **"Fantastic experience all-around. I cannot wait to take another course from SANS."**
>
> — Daniel Vandermark, **SUNY Oswego**

Train and Certify

SANS offers high-quality online cybersecurity training in two formats:

Live Online

- **Livestream instruction** by industry experts, along with hands-on labs
- **Real-time support** from teaching assistants and chat channels to network with peers
- **Free access to NetWars Tournaments** and online Capture-the-Flag events
- **Four months of access** to your class recordings to review topics on your own time

"The Live Online delivery platform ensures students are able to access content, virtual machines, labs, resources, and chat 24 hours a day....Additionally, after the course ends, access is still available! Priceless!!"

—Britni T., **U.S. Federal Agency**

&

OnDemand

- **Recorded instruction** by top practitioners
- **Hands-on labs and exercises** to test your skills during the course
- **Live chat** with GIAC-Certified subject-matter-expert support
- **Four months of online access** to your course on the OnDemand platform

"It's my first time taking an OnDemand course and I'm very impressed and satisfied. The platform is easy to use and the content is relatable."

—Scott Schroeder, **Western Area Power Administration**

Certify the Skills and Knowledge You Learn in SANS Training

Setting goals to learn new skills and pass a certification exam can be a challenging and rewarding personal experience. Proving to yourself that you can master skills and conquer the exam creates a sense of purpose. But GIAC Certifications go beyond just personal satisfaction. Research has shown that 82% of employers prefer hiring candidates with cybersecurity certifications, so by getting GIAC certified you confirm your own job security as well as the security of your enterprise.

"Now that I am certified, I feel that the whole 'Trust Me, I'm Certified' [notion] actually does exist. I was able to land my dream role thanks to the skills and knowledge I've learned via SANS courses and passing GIAC exams."

—Nate Gonzalez, GSEC, GCIH

sans.org/online

RETURN TO TABLE OF CONTENTS

Live Online

SANS Live Online training events provide instructor-led, interactive training with all the same additional learning opportunities as in-person events

Live Instruction by Expert Instructors

"Having a subject-matter-expert instructor with tons of real-world experience makes the course material easy to digest, and the Live Online platform is the best platform I've experienced!"
— Jeremy Swanson, **Mantech**

Interactive Courses with Hands-on Labs

"The combination of the instructor, classmates, written course materials, Live Online format, and interactive labs was outstanding. I would recommend SANS courses to anyone interested in a challenging and interactive learning atmosphere."
— William N., **U.S. Federal Government**

Real-Time Networking with Engaging Chat Channels

"I'm really happy with the interaction with the other students. This is my first Live Online course and I'm surprised at the proactive engagement of the students. I would have thought that you could only get that type of involvement from on-site/in-person course instruction."
— Sean Ayers, **UPS**

#hallway-david-bianco
Follow up with David after his talk in this channel
Cat Self 9:12 AM
oooooh I like that, Godfather of threat hunting, that
Matt Bromiley [SANS DFIR] 9:13 AM
image.png
YOU KNOW WHAT HURTS?
THE PYRAMID OF PAIN
Send a message to #hallway-david-bianco

"Having a dedicated moderator and teaching assistant in the Live Online classroom along with the instructor was an amazing help, and made me feel like SANS actually cares about my training experience. The dedicated online chat channel also allowed students to ask questions and get responses privately without disrupting the class!"
— James Murphy, **ARI**

sans.org/live-online

RETURN TO TABLE OF CONTENTS

OnDemand

Train at your own pace anytime, anywhere with SANS OnDemand

sans.org/ondemand

SANS OnDemand offers our world-class cybersecurity training in a self-paced online training format, with four months of extended access to your course and labs. Enjoy the ultimate learning flexibility with OnDemand – rewind and revisit your training content so you can reinforce the material and improve retention.

With complete control over the pace of learning, SANS OnDemand fits every learning style.

Why students choose OnDemand:

- Students can control the pace, learning environment, and schedule
- Instructor lectures, class exercises, and virtual labs are available for four months
- SANS subject-matter experts are on-hand and available to answer all of your questions
- Electronic, full-color courseware, materials, and course progress reports are provided for all courses
- Repeatable hands-on labs and quizzes help you prepare for 38 different GIAC exams

Limited-Time SANS Online Training Specials
Options include tablets, laptops, or discounts.
For more information visit: **sans.org/ondemand**

> "I don't think I would get nearly as much out of this course if I did not get the class material delivered via the OnDemand platform. It's an excellent way to replay content and critical topics."
> —Kenneth Huss, **Cisco**

> *"My GIAC certification doesn't mean I'm the fount of all security wisdom, but it does assure management that security concerns brought to their attention need serious consideration."*
>
> – Jenet Hensley,
> GCED, GWAPT, GSEC, GISP

GIAC develops and administers premier, professional cybersecurity certifications. Each certification aligns with SANS training and ensures mastery in critical, specialized InfoSec domains – providing the highest, most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world.

Learn more at GIAC.ORG

GIAC
The Highest Standard in Cybersecurity Certification

INTRODUCING

CYBERLIVE

Raising the bar even higher on GIAC Certifications

CyberLive brings real-world, virtual machine testing directly to cybersecurity practitioners, helping them prove their skills, abilities, and understanding – all in real-time.

Learn more at **giac.org/cyberlive**

> ***"Increasingly, the hands-on portion is important to measure the abilities of cyber professionals."***
>
> – Ben Boyle
> GXPN, GDAT, GWAPT

◀ RETURN TO TABLE OF CONTENTS

Courses/Events at a Glance

For an up-to-date course list, please check the website at sans.org/cyber-security-courses

			Page No.	OnDemand Available	GIAC Cert	Cloud Defender Jan 11 EST	Security East Jan 11 CST	Cyber Security Central: Jan Jan 18 CST	Cyber Threat Intelligence Summit & Training Jan 25 EST	Cyber Security West: Feb Feb 1 PST	Pen Test & Offensive Training Feb 8 CST	Open-Source Intelligence Summit & Training Feb 15 EST	Cyber Security East: Feb Feb 22 EST	Scottsdale: Virtual Edition Feb 22 MST	Cyber Security East: March Mar 1 EST	ICS Security Summit & Training Mar 8 EST	Cyber Security West: March Mar 15 PDT	SANS 2021 Mar 22 EDT	Leadership & Cloud Security Training Mar 29 EDT	Cyber Security Mountain: April Apr 5 MDT	Cyber Security East: April Apr 12 EDT	Pen Test Austin: Virtual Edition Apr 19 CDT	Baltimore Spring: Virtual Edition Apr 26 EDT	Rocky Mountain Spring: Virtual Edition Apr 26 MDT	Cyber Security Central: May May 3 CDT	DFIRCON Spring May 3 EDT	Security West May 10 PDT	Cyber Security East: May May 17 EDT	Purple Team Summit & Training May 17 EDT	Security Leadership: May May 24 CDT	CloudSec Next Summit & Training Jun 7 EDT	Cyber Security Central: June Jun 7 CDT	SOC Training Jun 14 EDT	Miami: Virtual Edition Jun 21 EDT	Cyber Security Mountain: June Jun 21 MDT	Security Leadership: June Jun 28 CDT
CYBER DEFENSE	SEC301	Introduction to Cyber Security	18	▶	GISF		301			301		301							301		301						301			301						301
	SEC401	Security Essentials Bootcamp Style	20	▶	GSEC		401		401	401		401		401	401		401	401		401	401		401		401		401	401				401	401		401	
	SEC450	Blue Team Fundamentals: Security Operations and Analysis	22	▶			450			450								450			450						450						450			
	SEC487	Open-Source Intelligence (OSINT) Gathering and Analysis	24	▶	GOSI				487			487						487			487						487		487				487			
	SEC501	Advanced Security Essentials – Enterprise Defender	26	▶	GCED		501							501				501			501			501			501					501				
	SEC503	Intrusion Detection In-Depth NEW!	28	▶	GCIA			503		503					503			503			503		503				503						503			
	SEC505	Securing Windows and PowerShell Automation	30	▶	GCWN					505								505									505					505				
	SEC511	Continuous Monitoring and Security Operations	32	▶	GMON		511			511					511			511			511						511						511			
	SEC530	Defensible Security Architecture and Engineering	34	▶	GDSA		530			530			530				530	530			530			530			530	530					530			
	SEC555	SIEM with Tactical Analytics	36	▶	GCDA				555					555				555			555						555						555			
	SEC573	Automating Information Security with Python	38	▶	GPYC						573							573				573					573						573			
OFFENSIVE OPERATIONS	SEC460	Enterprise and Cloud | Threat and Vulnerability Assessment NEW!	40	▶	GEVA			460			460							460				460					460								460	
	SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	42	▶	GCIH		504		504	504	504		504		504		504	504		504		504	504		504		504		504			504	504		504	
	SEC542	Web App Penetration Testing and Ethical Hacking	44	▶	GWAPT		542				542				542			542				542					542	542				542			542	
	SEC560	Network Penetration Testing and Ethical Hacking	46	▶	GPEN		560				560				560		560	560		560	560	560		560			560		560			560			560	
	SEC575	Mobile Device Security and Ethical Hacking	48	▶	GMOB						575							575				575												575		
	SEC588	Cloud Penetration Testing NEW!	50	▶	GCPN	588					588				588			588				588					588				588				588	
	SEC599	Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses	52	▶	GDAT		599		599					599				599				599					599		599				599			
	SEC617	Wireless Penetration Testing and Ethical Hacking	54	▶	GAWN						617							617				617						617								
	SEC642	Advanced Web App Pen Testing, Ethical Hacking & Exploitation Techniques NEW!	55	▶							642											642														
	SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	56	▶	GXPN		660				660		660					660				660					660						660			
	SEC699	Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection NEW!	58	▶			699				699							699				699							699						699	
	SEC760	Advanced Exploit Development for Penetration Testers	60	▶														760				760														
DFIR	FOR308	Digital Forensics Essentials NEW!	62	▶				308				308						308			308						308							308		
	FOR498	Battlefield Forensics & Data Acquisition	64	▶	GBFA					498					498			498		498						498								498		
	FOR500	Windows Forensic Analysis	66	▶	GCFE			500		500					500		500	500			500			500		500	500					500		500		
	FOR508	Advanced Incident Response, Threat Hunting, and Digital Forensics	68	▶	GCFA		508		508	508				508			508	508		508			508			508	508					508		508		
	FOR518	Mac and iOS Forensic Analysis and Incident Response	70	▶														518								518										
	FOR572	Advanced Network Forensics: Threat Hunting, Analysis & Incident Response	72	▶	GNFA		572		572					572				572		572						572	572					572		572		
	FOR578	Cyber Threat Intelligence	74	▶	GCTI				578			578					578				578					578								578		
	FOR585	Smartphone Forensic Analysis In-Depth	76	▶	GASF			585										585								585										
	FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	78	▶	GREM				610					610				610		610						610						610				
MANAGEMENT	MGT414	SANS Training Program for CISSP® Certification	80	▶	GISP		414			414				414				414			414			414			414							414		
	MGT512	Security Leadership Essentials for Managers	82	▶	GSLC		512			512			512				512		512		512		512				512			512			512			512
	MGT514	Security Strategic Planning, Policy, and Leadership	84	▶	GSTRT		514							514					514		514				514		514			514						514
	MGT516	Managing Security Vulnerabilities: Enterprise and Cloud NEW!	86	▶		516								516					516			516					516				516				516	
	MGT521	Leading Cybersecurity Change: Building a Security-Based Culture NEW!	88					521											521											521						521
	MGT525	IT Project Management and Effective Communication	90	▶	GCPM													525									525									
	SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	92	▶	GCCC			566											566	566										566						566
	AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	94	▶	GSNA												507																			
	LEG523	Law of Data Security and Investigations	95	▶	GLEG														523								523									523
CLOUD	SEC488	Cloud Security Essentials NEW!	96		GCLD	488				488			488					488			488			488			488	488			488				488	
	SEC510	Public Cloud Security: AWS, Azure, and GCP NEW!	98											510					510				510				510				510					
	SEC522	Defending Web Applications Security Essentials	100	▶	GWEB	522											522							522							522					
	SEC540	Cloud Security and DevOps Automation	102	▶	GCSA	540				540				540					540		540		540				540				540				540	
	SEC545	Cloud Security Architecture and Operations	104	▶		545				545				545					545				545		545			545			545					
ICS	ICS410	ICS/SCADA Security Essentials	106	▶	GICSP		410			410						410							410									410				
	ICS456	Essentials for NERC Critical Infrastructure Protection	108	▶	GCIP		456									456																456				
	ICS515	ICS Active Defense and Incident Response	110	▶	GRID		515		515							515							515									515				
NETWARS		Core NetWars Tournament	16				Core				Core						Core	Core				Core	Core				Core						Core			
		Cyber Defense NetWars Tournament	16					CD							CD			CD									CD						CD			
		DFIR NetWars Tournament	16						DFIR									DFIR		DFIR						DFIR						DFIR				
		Grid NetWars Tournament	16				Grid									Grid																				

◀ RETURN TO TABLE OF CONTENTS

What's New!

2021 Virtual Summits

FREE for the Global Community

Double down on your training goals, learn new cybersecurity skills, and forge new industry connections in 2021 at any or all of these upcoming Summits.

> "The free, Live Online Summits this year were a welcomed way to get high-quality knowledge, inspiration, and networking while working remotely. It enabled me to share training opportunities and experiences with teammates that I would not have been able to share otherwise."
>
> — Jen Fox, Information Security Program Specialist

> "I have been blown away by SANS' ability to quickly pivot to online events, while maintaining the quality and community flavor of its in-person events in 2020."
>
> — Christina Morillo, Sr. Product Manager, Security

Upcoming SANS Summit & Training Events

Cyber Threat Intelligence

SUMMIT: Jan 21–22 | TRAINING: Jan 25–30

Open-Source Intelligence

SUMMIT: Feb 11–12 | TRAINING: Feb 8–10 & 15–20

ICS Security

SUMMIT: Mar 4–5 | TRAINING: Mar 8–13

Purple Team

SUMMIT: May 24–25 | TRAINING: May 17–22

CloudSec Next

SUMMIT: Jun 3–4 | TRAINING: Jun 7–12

DFIR

SUMMIT: Jul 22–23 | TRAINING: Jul 26–31

View the Summit calendar and get registered at **sans.org/summit**

RETURN TO TABLE OF CONTENTS

SANS Faculty

SANS Instructors are a select group of highly skilled practitioners who have earned respect and recognition as being among the top minds in cybersecurity. Not only have these individuals proven their expertise in the field, they have demonstrated extraordinary ability to train others to advance their own capabilities.

SANS Faculty at a Glance

120+ Instructors

Each of our 120+ certified instructors is a highly skilled professional currently working in cybersecurity.

16+ Years

SANS faculty spend an average of more than 16 years as cybersecurity practitioners before being selected to become SANS Certified Instructors.

40+ Books

SANS faculty members have authored more than 40 books on information security.

150+ Tools

More than 150 open-source cybersecurity tools have been created by SANS Instructors. List of tools available at **sans.org/free**.

3,500+ Resources

SANS faculty members have produced more than 3,500 research papers and webcasts on information security topics.

Commitment

SANS instructors are committed to providing engaging and positive active learning environments that focus on key skills taught through lectures, immersive hands-on labs, and interactive discussions. Passionate is a word many use to describe being taught by a Certified SANS Instructor.

Their goal is your success, and **we promise that you will be able to apply what you learn as soon as you return to work.**

Meet the SANS faculty: **sans.org/instructors**

STAY SHARP

High-Impact Cybersecurity Training

Stay Sharp with 1-, 2-, and 3-Day Courses

With the convergence of work responsibilities and home life, many cybersecurity professionals struggle to find the time to advance their skills.

That's why we've created the SANS Stay Sharp Series of short courses. This new series of 1- to 3-day courses will equip your team with in-depth technical knowledge and specific job skills for critical cybersecurity focus areas.

Whether you manage a team of seasoned professionals or new cyber recruits, SANS Stay Sharp training is the perfect way to quickly build practical cyber skills that will get the job done.

> *"The content squeezed into two days is more than I could have learned on my own in six months. The resources and materials shared are going to be hugely valuable."*
>
> — Benedict Donaldson, **Dyson**

What Are SANS Stay Sharp Short Courses?

- SANS' high-quality training delivered over 1, 2, or 3 days
- Targeted for specific technical knowledge and skills
- Virtual training delivered Live Online
- Instructor-led courses featuring the world's leading cybersecurity professionals
- Four months of access to the recorded course lectures

STAY SHARP

Blue Team Operations

SEC455: SIEM Design & Implementation (2 DAYS)

SEC455 is an important primer to those who are unfamiliar with the architecture of an elastic-based SIEM. Students who have taken or plan to take additional cyber defense courses will find SEC455 to be a helpful supplement to the advanced concepts they will encounter in courses such as SEC555.

NEW! **SEC537: Practical OSINT Analysis and Automation** (2 DAYS)

This course teaches practical open-source intelligence (OSINT) analysis and automation techniques. You will learn tradecraft tips, tactics, techniques, and procedures based on real-world examples that will enable you to carry out in-depth OSINT analysis of groups, image and video verification, and OSINT operations security, as well as understand the foundations of automating OSINT with Python.

NEW! **SEC582: Mastering TShark Packet Analysis** (2 DAYS)

With SEC582, you will master performing packet analysis through TShark and learn how to solve real-world problems through 19 different labs, demos, and challenges. This is the most in-depth, hands-on packet analysis course available through SANS.

NEW! **SEC583: Crafting Packets** (1 DAY)

SEC583 is a lab-heavy course designed to teach the powerful skill of how to craft and manipulate packets. This skill can be used to test policies, behaviors, and configurations and will also provide deeper understanding of TCP/IP and application protocols.

STAY SHARP

Offensive Operations

NEW! **SEC552: Bug Bounties and Responsible Disclosure** (2 DAYS)

SEC552 teaches students how to apply modern attack techniques inspired by real-world bug bounty case studies. This course provides a methodology to discover and responsibly disclose tricky, logic-based application flaws that automated scanning tools do not reveal.

NEW! **SEC554: Blockchain and Smart Contract Security** (3 DAYS)

SEC554 will teach you the essential topics of blockchain and smart contract technology. The course takes a detailed look at the cryptography and transactions behind blockchain and provides the hands-on training and tools to deploy, audit, scan, and exploit blockchain and smart contract assets.

SEC564: Red Team Exercises and Adversary Emulation (2 DAYS)

SEC564 provides students with the skills to plan and manage Red Team Exercises. Students will learn the tactics, techniques, and procedures (TTPs) used by the adversary, then create an adversary emulation plan leveraging the MITRE ATT&CK (Adversary Tactics, Techniques, and Common Knowledge) framework.

SEC580: Metasploit Kung Fu for Enterprise Pen Testing (2 DAYS)

SEC580 will teach you how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen. You will learn how Metasploit can fit into your day-to-day penetration testing assessment activities. You'll gain an in-depth understanding of the Metasploit Framework far beyond how to exploit a remote system.

◀ RETURN TO TABLE OF CONTENTS

What's New!

STAY SHARP

STAY SHARP

Cybersecurity Leadership

MGT415: A Practical Introduction to Cyber Security Risk Management (2 DAYS)

MGT415 will provide students with an introduction to thinking practically about risk management and teach the skills necessary to perform risk assessments. Not only will students learn foundational concepts of risk, but they will be given templates and tools that they can take back to their office immediately after class to perform risk assessments. Throughout the class students will learn introductory concepts of Governance, Risk, and Compliance (GRC) that they can use to mature their cybersecurity programs.

NEW! **MGT433: Managing Human Risk: Mature Security Awareness Programs (2 DAYS)**

Learn the key lessons and roadmap to building a mature awareness program that your workforce will love and that has an impact you can measure. You'll apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, Golden Circle and learn about the Elephant vs. the Rider.

NEW! **MGT520: Leading Cloud Security Design and Implementation (2 DAYS)**

MGT520 teaches students how to build, lead, and implement a cloud security transition plan and roadmap, and then execute and manage ongoing operations. An organization's cloud transition requires numerous key decisions. This course provides the information security leaders need to drive a secure cloud model and leapfrog on security by leveraging the security capabilities in the cloud.

NEW! **MGT551: Building and Leading Security Operations Centers (2 DAYS)**

Looking to build, manage, or improve your Security Operations Center? The brand new MGT551 is the course for you! With lessons from those who have been in the trenches for years, this hands-on course will help you define, implement and sharpen your organization's cyber defense, and show you how to implement those tactics using the industries best free and open-source tools!

SEC440: Critical Security Controls: Planning, Implementing, and Auditing (2 DAYS)

For security professionals, this course enables you to see how to put the controls in place in your existing network though effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. The course draws heavily on the Top 20 Critical Security Controls.

NEW! **SEC474: Building a Healthcare Security & Compliance Program (2 DAYS)**

Healthcare organizations in the United States face two major challenges: first, to properly secure the organization from tactical risk, and second, to achieve compliance with the array of government regulations known as HIPAA. This course will help students develop the skills to make measurable improvements to the overall security posture of their organization's IT infrastructure while also building and maintaining a compliance program. Using the safeguards of the HIPAA Security Rule along with the NIST Framework 800-66 to identify and assess risk, students will learn how to report progress on their compliance activities and their security value in support of the organization's mission.

> *"With SANS, I know I am getting the best information security training in the industry, and that continues to be the case with SANS Live Online!"*
>
> — Harold (Chip) Stockton, **Global Payments, Inc.**

STAY SHARP

Cloud Security

SEC534: Secure DevOps: A Practical Introduction (2 DAYS)

This course explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn DevOps principles, practices, and tools and how they can be leveraged to improve the reliability, integrity, and security of systems.

NEW! **SEC541: Cloud Security Monitoring and Threat Detection (1 DAY)**

SEC541 will take you on a deep dive into Amazon Web Services (AWS) in order to search out and identify threats in your cloud environment. We will look at the most common threat techniques used against AWS environments, what their characteristics are, and how to detect them.

NEW! **SEC584: Cloud Native Security: Defending Containers and Kubernetes (3 DAYS)**

SEC584 will perform a deep dive into defending key infrastructure deployment components, focusing on containerization and orchestration exploits. Students will be thrust directly into detailed issues related to misconfiguration and known attack patterns and will learn how to properly harden and protect against these exploits.

STAY SHARP

Digital Forensics & Incident Response

NEW! **FOR498A: Battlefield Acquisition (3 DAYS)**

FOR498A teaches the latest tools, digital container access techniques, and enterprise methodologies to identify, access, and preserve evidence across a vast range of devices, repositories, and non-traditional storage areas. Learn how to extract actionable intelligence in 90 minutes or less.

NEW! **FOR498T: Triage and Early Analysis (3 DAYS)**

FOR498T teaches you how to perform a very rapid triage collection that can be used to start your investigation sooner. You will be equipped to work in less-than-optimal surroundings, identify all necessary data and collect the data in a properly defensible manner, and maintain the integrity of the data.

NEW! **FOR508A: Anti-Forensics Detection & Analysis (2 DAYS)**

FOR508A explores a variety of deep-dive techniques that forensic analysts can use to uncover hidden evidence of malicious behavior on Windows systems, whether it be from a network intruder, a malicious insider, or a criminal suspect.

NEW! **FOR572L: Lethal Network Forensics (2 DAYS)**

FOR572L teaches the three primary sources of network-based evidence: full packet capture, NetFlow, and logs. Whether used together or separately, or in conjunction with host-based evidence or alone, these sources can provide critical insight into the actions attackers have taken or continue to take in their victims' environment.

NEW! **FOR585A: Android Forensic Analysis (2 DAYS)**

FOR585A teaches what you can recover from Android devices using digital forensic methodologies and provides approaches for dealing with challenges such as encryption, passwords, and interpretation of artifacts. This course will prepare you for the rapidly evolving world of smartphone forensics.

NEW! **FOR585I: iOS Forensic Analysis (2 DAYS)**

FOR585I teaches the proper handling and parsing skills needed to bypass locked iOS devices and correctly interpret the data. It delves into the iOS file system and discusses common areas containing files of evidentiary value. This course will prepare you to deal with the iOS device that will likely be a major component in a forensic investigation.

NEW! **FOR610L: Lethal Malware Analysis (2 DAYS)**

FOR610L supercharges your incident response and forensics skills by teaching you how to use key malware analysis tools and techniques. This practical, hands-on course builds upon your existing network, system and InfoSec skills and teaches you how to turn Windows and related malware inside out.

◀ RETURN TO TABLE OF CONTENTS

STAY SHARP

	JAN	FEB	MAR	APR	MAY	JUN
SEC440: Critical Security Controls: Planning, Implementing & Auditing		3–4 (CST)	31 – Apr 1 (EDT)			28–29 (CDT)
SEC455: SIEM Design & Implementation	18–19 (MST)	9–10 (EST)				28–29 (CDT)
SEC474: Building A Healthcare Security & Compliance Program		1–2 (CST)				28–29 (CDT)
SEC520: Leading Cloud Security Design and Implementation		16–17 (EST)	31 – Apr 1 (EDT)			1–2 (EDT) 28–29 (CDT)
SEC534: Secure DevOps: A Practical Introduction	14–15 (EST)	1–2 (CST)				1–2 (EDT)
SEC537: Practical Open-Source Intelligence (OSINT) Analysis and Automation	18–19 (MST)	15–16 (EST)			26–27 (EDT)	28–29 (CDT)
SEC541: Cloud Security Monitoring and Threat Detection		1 (CST)	29 (EDT)			2 (EDT)
SEC552: Bug Bounties and Responsible Disclosure		8–9 (CST)	8–9 (EST)	19–20 (CDT)	26–27 (EDT)	
SEC554: Blockchain and Smart Contract Security		10–12 (CST)				
SEC564: Red Team Exercises and Adversary Emulation		10–11 (CST)	8–9 (EST)	19–20 (CDT)	26–27 (EDT)	
SEC580: Metasploit Kung Fu for Enterprise Pen Testing		8–9 (CST)	8–9 (EST)	19–20 (CDT)		
SEC582: Mastering TShark Packet Analysis	19–20 (MST)	9–10 (EST)			27–28 (EDT)	28–29 (CDT)
SEC583: Crafting Packets	18 (MST)	8 (EST)			26 (EDT)	28 (CDT)
SEC584: Cloud Native Security: Defending Containers & Kubernetes		1–3 (CST)				7–9 (EDT)
FOR498A: Battlefield Acquisition				5–7 (CDT)	3–5 (EDT)	
FOR498T: Triage and Early Analysis				5–7 (CDT)	3–5 (EDT)	
FOR508A: Anti-Forensics Detection & Analysisn				5–6 (CDT)	3–4 (EDT)	
FOR572L: Lethal Network Forensics				5–6 (CDT)	3–4 (EDT)	
FOR585A: Android Forensic Analysis				5–6 (CDT)	3–4 (EDT)	
FOR585I: iOS Forensic Analysis				5–6 (CDT)	3–4 (EDT)	
FOR610L: Lethal Malware Analysis				5–6 (CDT)	3–4 (EDT)	
MGT415: A Practical Introduction to Cyber Security Risk Management		3–4 (CST)	31 – Apr 1 (EDT)			28–29 (CDT)
MGT433: Managing Human Risk: Mature Security Awareness Programs		1–2 (CST)	20–30 (EDT)			28–29 (CDT)
MGT551: Building and Leading Security Operations Centers		3–4 (CST)	29–30 (EDT)			

◀ RETURN TO TABLE OF CONTENTS

Want to launch a career in cybersecurity?

Earn an Undergraduate Certificate in Applied Cybersecurity

Gain fundamental technical knowledge and skills, choose an elective course to begin developing a specialized skillset, and earn GIAC certifications that employers are looking for.

Rapid Career Preparation

Complete the program in 18 months or choose an accelerated option to finish in less than a year. 91% of graduates are employed in cybersecurity within 6 months.

Flexibility

Pursue the certificate alongside a degree program or while working full-time. A 100% online option is available.

> *"I was having a hard time getting a job in information security due to my lack of hands-on experience. SANS gave me extraordinary training and the opportunity to rise to the top of the résumé pile."*
>
> – AJ Langlois
> *Cyber Analyst II, BB&T*

SANS
Technology
Institute

A Curriculum Designed to Launch Careers in Cybersecurity

Security Foundations

SEC 401 | GSEC Certification

SEC 504 | GCIH Certification

Elective Course | GIAC Certification

New to the field? No problem.

Prior cybersecurity experience isn't needed, but you must have completed at least 2 years of college.

The SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education (3624 Market Street, Philadelphia, PA 19104 - 267.284.5000), an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

SANS.edu/acs

SANS **Cyber Ranges**

sans.org/cyber-ranges

A Continuum of Hands-On Learning

SANS offers a comprehensive suite of hands-on ranges with industry-leading interactive learning scenarios:

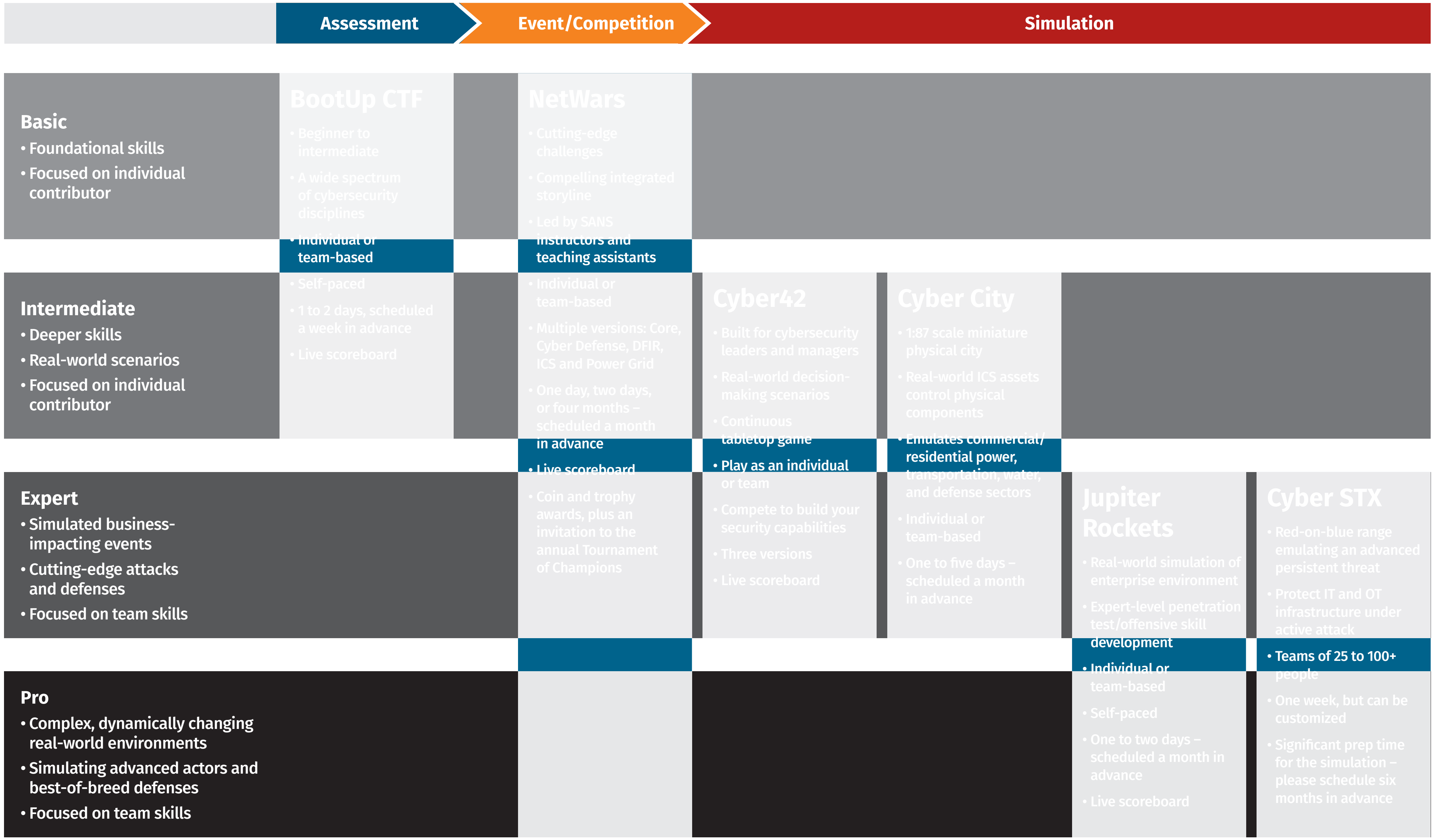
- Develop and practice the real-world cybersecurity skills your team needs
- Available online or in-person, any time, anywhere

Why Utilize SANS Cyber Ranges?

- SANS is the most trusted name in cybersecurity
- World-class SANS instructors create our Cyber Ranges for all skill levels
- SANS Cyber Ranges can help your team assess candidates, build useful skills, and simulate real-world scenarios
- Your team memberswill be able to apply what they learn on SANS Cyber Ranges as soon as they return to work
- An ideal way to invest in your team's skills, enhancing retention and preparing team members to defend your environment

> *"NetWars is challenging for all levels of expertise, has great hints if you get stuck, and promotes continuous education."*
>
> — Jon-Michael Lacek, **Wegmans Food Markets**

> *"Core NetWars was challenging but not frustrating for newbies. This is my first time doing NetWars and it has been a blast."*
>
> — Rachael Murray, **Northwestern Mutual**



Assessment | Event/Competition | Simulation

Basic
- Foundational skills
- Focused on individual contributor

Intermediate
- Deeper skills
- Real-world scenarios
- Focused on individual contributor

Expert
- Simulated business-impacting events
- Cutting-edge attacks and defenses
- Focused on team skills

Pro
- Complex, dynamically changing real-world environments
- Simulating advanced actors and best-of-breed defenses
- Focused on team skills

BootUp CTF
- Beginner to intermediate
- A wide spectrum of cybersecurity disciplines
- Individual or team-based
- Self-paced
- 1 to 2 days, scheduled a week in advance
- Live scoreboard

NetWars
- Cutting-edge challenges
- Compelling integrated storyline
- Led by SANS instructors and teaching assistants
- Individual or team-based
- Multiple versions: Core, Cyber Defense, DFIR, ICS and Power Grid
- One day, two days, or four months – scheduled a month in advance
- Live scoreboard
- Coin and trophy awards, plus an invitation to the annual Tournament of Champions

Cyber42
- Built for cybersecurity leaders and managers
- Real-world decision-making scenarios
- Continuous tabletop game
- Play as an individual or team
- Compete to build your security capabilities
- Three versions
- Live scoreboard

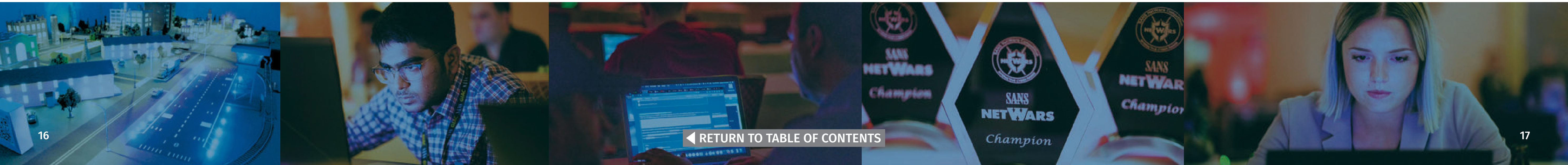
Cyber City
- 1:87 scale miniature physical city
- Real-world ICS assets control physical components
- Emulates commercial/residential power, transportation, water, and defense sectors
- Individual or team-based
- One to five days – scheduled a month in advance

Jupiter Rockets
- Real-world simulation of enterprise environment
- Expert-level penetration test/offensive skill development
- Individual or team-based
- Self-paced
- One to two days – scheduled a month in advance
- Live scoreboard

Cyber STX
- Red-on-blue range emulating an advanced persistent threat
- Protect IT and OT infrastructure under active attack
- Teams of 25 to 100+ people
- One week, but can be customized
- Significant prep time for the simulation – please schedule six months in advance

Powered by SANS

For custom Cyber Range options and the schedule of upcoming Community CTF events and NetWars Tournaments, visit **sans.org/cyber-ranges**



RETURN TO TABLE OF CONTENTS

SEC301: **Introduction to Cyber Security**

GISF
Information Security Fundamentals
giac.org/gisf

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) for prioritization of critical security resources
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand how a computer works
- Understand computer network basics
- Have a fundamental grasp of any number of technical acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS, and the list goes on.
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, intrusion detection systems, sniffers, ethical hacking, active defense, and threat hunting.
- Understand wireless technologies including WiFi, Bluetooth, mobile phones and the Internet of Things (IoT)
- Explain a variety of frequent attacks such as social engineering, drive-by downloads, watering hole attacks, lateral movement, and other attacks
- Understand different types of malware
- Understand browser security and the privacy issues associated with web browsing
- Explain system hardening
- Discuss system patching
- Understand virtual machines and cloud computing
- Understand backups and create a backup plan for your personal life that virtually guarantees you never have to pay ransom to access your data

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Are you new to cybersecurity and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Do you need to be conversant in basic security concepts, principles, and terms, but do not need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training/certification?
- Are you a manager who lays awake at night worrying that your company may be the next mega-breach headline story on the 6 o'clock news?

If you answer yes to any of these questions, the SEC301: Introduction to Cyber Security training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to cybersecurity.

This five-section comprehensive course covers everything from core terminology to how computers and networks function, security policies, risk management, a new way of looking at passwords, cryptographic principles, network attacks and malware, wireless security, firewalls and many other security technologies, web and browser security, backups, virtual machines and cloud computing. All topics are covered at an easy to understand introductory level.

This course is for those who have very little knowledge of computers and technology with no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach enables you to grasp all the information presented, even if some of the topics are new to you. You'll learn real-world cybersecurity fundamentals to serve as the foundation of your career skills and knowledge for years to come.

Written by a cybersecurity professional with over 35 years of industry experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as getting you ready for your next training course. It also delivers on the SANS promise: "You can use the knowledge and skills you learn in SEC301 as soon as you return to work."

> **"SEC301 provided a great foundation for the topic of security, since I deal with it on a daily basis."**
>
> — Richard Pollich, **Broadridge Financial Solutions Inc.**

SEC301: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Security's Foundation

Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first section, you will fully understand the Principle of Least Privilege and Confidentiality, Integrity, Availability (CIA), and you'll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, and authentication/authorization/accountability.

SECTION 3: An Introduction to Cryptography

Cryptography is one of the most complex issues faced by security practitioners. It is not a topic you can explain in passing; we spend a full day on it. You do not need a calculator for this course section since we do not delve into the math behind crypto. We introduce you to cryptographic terms. We explain what steganography is. We then look at historical examples of cryptography. We do this because even the most advanced cryptographic systems today utilize methods of encrypting data that were used hundreds of years B.C. So we explain the historical examples that are very easy to understand to make it easier to understand modern cryptographic methods and principles. We cover the "work factor" – the length of time necessary to break cryptography and why understanding this concept is so important. We cover some of the potential attacks against crypto and which ones are viable against modern cryptography and which attacks are nonviable. We cover hashing, symmetric and asymmetric cryptography and how each works. We then show real-world examples of how those cryptographic systems work. We cover the secure key exchange mechanism called Diffie-Hellman. We even briefly cover digital certificates and Public Key Infrastructure (PKI). Once we have thoroughly explained how cryptography works, we end the section with a discussion of data encrypting protocols. We'll look at what uses cryptography to secure data on our networks and across the Internet. Here we cover email encryption, secure remote administration, secure file transfer, and three examples of Virtual Private Networks (VPNs).

SECTION 2: Computer Functions and Networking

The course begins with a discussion of how computers work. We cover the numbering system of decimal, binary, and hexadecimal – vital to understanding computers and networks. We also cover ASCII (the American Standard Code for Information Interchange). We also discuss what an operating system is. We talk about the terms kilobyte, megabyte, gigabyte, and terabyte and what those terms mean. We cover the difference between the hard drive and Random Access Memory (RAM). From there, we move to a discussion of how information moves from point A to point B across a network without using any technical terminology of any kind. This discussion includes both Internet and Local Area Network (LAN) examples. As we move on through the course section, we slowly add the technical aspects of those explanations, including the terms and acronyms of networking. We discuss the origins of the Internet and why that origin matters to modern-day cybersecurity. We explain what a protocol is, and what both the OSI and TCP/IP stacks are and why they matter. You learn about standard network hardware such as a network interface card, a switch, and a router. We progress to topics such as IP addresses, network masks, default gateways, and routing. We explain, compare, and contrast the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) and why you might want to use one over the other. Eventually, we get to network protocols such as the Dynamic Host Control Protocol (DHCP), Domain Name System (DNS), and Network Address Translation (NAT). While the above description sounds exceptionally technical, rest assured that we present the material in the most non-technical way possible. We cover each topic at a very high level without getting into the nitty-gritty details.

SECTION 4: Cybersecurity Technologies – Part 1

Our fourth section in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (WiFi and Bluetooth) and mobile device security (i.e., mobile phones and tablets). We compare and contrast the security models of Apple's iPhone and Google's Android phones. We also discuss the almost total lack of security in the Internet of Things (IoT). We follow that with a look at some frequent attacks, including open-source intelligence gathering, social engineering, drive-by download attacks, watering hole attacks, buffer overflow attacks, Denial of Service (DoS), and other frequent attacks. We then move into a discussion of malware. What is a virus versus a worm or a trojan horse? What is ransomware, and what is cryptojacking. We then cover both anti-malware and host firewalls that try to counter these problems.

SECTION 5: Cybersecurity Technologies – Part 2

The final section of our SEC301 journey continues the discussion of cybersecurity technologies. The course section begins by looking at several security technologies, including compartmentalization, firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), sniffers, content filters, sinkholes, ethical hacking, active defense, threat hunting and many more. We then take a solid look at browser and web security, and the difficulties of securing the web environment. For example, students understand why and how their browser connects to anywhere from 5 to 100+ different Internet locations each time they load a single web page. We end the section with a look at system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup. We include solid real-world examples of how to implement these.

Who Should Attend

- Anyone new to cybersecurity and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don't understand, but want to understand
- Professionals who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification
- Managers who worry their company may be the next mega-breach headline story on the 6 o'clock news

> **"SEC301 is a great class for the individual who wants to learn an extensive amount of material in one week."**
>
> — Steven Chovanec,
> **Discover Financial Services**

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
OSINT Summit	Feb 15
Leadership & Cloud Security	Mar 29
Cyber Security East: April	Apr 12
Security West	May 10
Security Leadership: May	May 24
Security Leadership: June	Jun 28

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

◀ RETURN TO TABLE OF CONTENTS

SEC401: **Security Essentials Bootcamp Style**

GSEC
Security Essentials
giac.org/gsec

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Develop effective security metrics that provide a focused playbook that the IT department can implement, auditors can validate, and executives can understand
- Analyze the risk to your environment in order to drive the creation of a security roadmap that focuses on the right areas of security
- Make use of practical tips and tricks that focus on addressing high-priority security problems within your organization and doing the right things that lead to security solutions that work
- Understand why some organizations win and why some lose when it comes to security and, most importantly, how to be on the winning side
- Understand the core areas of security and how to create a security program that is built on a foundation of Detection, Response, and Prevention

> **"SEC401 is a great intro and overview of network security. It covered just enough information to get a baseline level of knowledge without going too in-depth on any one topic."**
>
> — Josh Winter, **Washington County, MN**

> **"SEC401 provides an excellent overview of security fundamentals delivered by experienced industry professionals."**
>
> — Jason W., **U.S. Federal Agency**

This course will show you the most effective steps to prevent attacks and detect adversaries with actionable techniques that can be used as soon as you get back to work. You'll learn tips and tricks designed to help you win the battle against the wide range of cyber adversaries that want to harm your environment.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

SEC401 provides you with the information security knowledge needed to help you answer these questions for your environment, delivered in a bootcamp-style format reinforced with hands-on labs.

LEARN TO BUILD A SECURITY ROADMAP THAT CAN SCALE TODAY AND INTO THE FUTURE

SEC401: Security Essentials Bootcamp Style is focused on providing you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. The course will show you how to prevent your organization's security problems from becoming headline news in the *Wall Street Journal*!

PREVENTION IS IDEAL BUT DETECTION IS A MUST

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

All in all, however, organizations are going to be targeted AND broken into. Today, more than ever before, TIMELY detection and response are critical. Once an adversary is inside the environment, damage will occur. In the near future, the key question in information security will become, "How quickly can we detect, respond, and remediate an adversary?" As counterintuitive as it may seem, it needs to be stated that you CANNOT secure what you don't know you have. Security is all about making sure you focus on the right areas of defense (especially as applied to the uniqueness of YOUR organization). In SEC401 you will learn the language and underlying workings of computer and information security, and how best to apply it to your unique needs. You will gain the essential and effective security knowledge you will need if you are given the responsibility to secure systems and/or organizations.

SEC401: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Network Security Essentials

A key way that attackers gain access to a company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered in this first section in order to provide a firm foundation for the consecutive sections of training.

Topics: SEC401 – An Introduction; Defensible Network Architecture; Networking and Protocols; Network Device Security; Virtualization and Cloud Security; Securing Wireless Networks

SECTION 3: Vulnerability Management and Response

In Section 3, our focus shifts to the various areas of our environment where vulnerabilities manifest. We will begin with an overall discussion of exactly what constitutes a vulnerability, and how to best implement a proper vulnerability assessment program. Penetration testing is often discussed in concert with vulnerability assessment, even though vulnerability assessment and penetration testing are quite distinct from each other.

Topics: Vulnerability Assessments; Penetration Testing; Attacks and Malicious Software; Web Application Security; Security Operations and Log Management; Digital Forensics and Incident Response

SECTION 5: Windows Security

Remember when Windows was simple? Windows XP desktops in a little workgroup...what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure, and so on. Microsoft is battling Google, Apple, Amazon, and other cloud giants for cloud supremacy. The trick is to do cloud securely, of course. Windows is the most widely used and targeted operating system on the planet. At the same time, the complexities of Active Directory, Public Key Infrastructure, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. Section 5 will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the section with a solid grounding in Windows security by looking at automation, auditing, and forensics.

Topics: Windows Security Infrastructure; Windows as a Service; Windows Access Controls; Enforcing Security Policy; Network Services and Cloud Computing; Automation, Auditing, and Forensics

SECTION 2: Defense-In-Depth

To secure an enterprise network, you must understand the general principles of network security. In Section 2, we look at the "big picture" threats to our systems and how to defend against them. We will learn that protections need to be layered leveraging a principle called defense-in-depth, and then explain the principles that will serve us well in protecting our systems.

Topics: Defense-in-Depth; Identity and Access Management; Authentication and Password Security; Center for Internet Security (CIS) Controls; Data Loss Prevention; Security Plans and Risk Management

SECTION 4: Data Security Technologies

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, although few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. During the first half of Section 4 we'll look at various aspects of cryptographic concepts and how they can be used in securing an organization's assets. A related discipline called steganography, or information hiding, is also covered. During the second half of the section, we shift our focus to the various types of prevention technologies that can be used to stop an adversary from gaining access to our organization (firewalls, intrusion prevention systems) and the various types of detection technologies that can detect the presence of an adversary on our networks (intrusion detection systems). These preventative and detective techniques can be deployed from a network and/or endpoint perspective; the similarities and differences in the application of these techniques will be explored.

Topics: Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Network Security Devices; Endpoint Security

SECTION 6: Linux, Mac, and Smartphone Security

While organizations do not have as many Linux systems, the Linux systems that they do have are often some of the most critical systems that need to be protected. Section 6 provides guidance to improve the security of any Linux system. The section combines practical "how to" instructions with background information for Linux beginners, as well as security advice and best practices for administrators with various levels of expertise. With the idea of Linux being a 'free' operating system, it isn't a surprise that many advanced security concepts are first developed for Linux. Containers is one example. Containers provide powerful and flexible concepts for cloud computing deployments. While not specifically designed for information security purposes, containers are built on elements of minimization and that is something we can leverage in an overall information security methodology (as a part of defense-in-depth). What containers do and do not represent for information security, and the best practice for their management, will be fully discussed. A discussion of Linux and UNIX concepts would not be complete without a discussion of the macOS (which is based on UNIX). Apple's venerable macOS provides extensive opportunity for hardware and software security but is often misunderstood in terms of what can and cannot be achieved. Because most of our modern-day mobile operating systems have a Linux and/or UNIX background, we end our Section 6 with a discussion on mobile device security.

Topics: Linux Security: Structure, Permissions, and Access Controls; Hardening and Securing Linux Services; Monitoring and Attack Detection; Security Utilities

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
CTI Summit	Jan 25
Cyber Security West: Feb	Feb 1
OSINT Summit	Feb 15
Scottsdale: Virtual Edition	Feb 22
Cyber Security East: March	Mar 1
Cyber Security West: March	Mar 15
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
Cyber Security East: April	Apr 12
Baltimore Spring: Virtual Edition	Apr 26
Cyber Security Central: May	May 3
Security West	May 10
Cyber Security East: May	May 17
Cyber Security Central: June	Jun 7
SOC Training	Jun 14
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC450: **Blue Team Fundamentals: Security Operations and Analysis**

6 Day Program	36 CPEs	Laptop Required

Who Should Attend

- Security analysts
- Incident investigators
- Security engineers and architects
- Technical security managers
- Security Operations Center (SOC) managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC
- Anyone looking to start their career on the blue team

Course Author Statement

"As someone who has held every position from entry-level analyst to SOC manager at a 100,000-employee company, I thoroughly understand the struggle of starting your first position in cyber defense. While there is a seemingly infinite amount of information to learn, there are certain central concepts that, when explained systematically, can greatly shorten the time required to become a productive member of the team. This course was written to pass this knowledge on to you, giving you both the high- and low-level concepts required to propel your career in cyber defense. It's packed with the concepts that I expected new employees to understand, as well the thought process we tried to cultivate throughout analysts' careers to ensure the success of the individual and the organization."
— John Hubbard

Is your organization looking for a quick and effective way to onboard new security analysts, engineers, and architects? Do your Security Operations Center (SOC) managers need additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC?

SEC450 is an accelerated on-ramp for new cyber defense team members and SOC managers. This course introduces students to the tools common to a defender's work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know.

Students will learn the stages of security operations: how data is collected, where it is collected, and how threats are identified within that data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

The course employs practical, hands-on instruction using a simulated SOC environment with a real, fully-integrated toolset that includes:

- Security Information and Event Management (SIEM)
- An incident tracking and management system
- A threat intelligence platform
- Packet capture and analysis
- Automation tools

While cyber defense can be a challenging and engaging career, many SOCs are negatively affected by turnover. To preemptively tackle this problem, this course also presents research-backed information on preventing burnout and how to keep engagement high through continuous growth, automation, and false positive reduction. Students will finish the course with a full-scope view of how collection and detection work, how SOC tools are used and fit together, and how to keep their SOC up and running over the long term.

> **"Visualizing logs and understanding how they go to SIEM was super helpful, especially for someone about to become a SIEM admin. Malware Analysis portion was fantastic for analysts at every level."**
>
> — Troy Dinkel, **Aires**

SEC450: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Blue Team Tools and Operations

This section starts with an introduction to the blue team, the mission of a SOC, and how to understand an organization's threat model and risk appetite. It is focused on top-down learning to explain the mindset of an analyst, the workflow, and monitoring tools used in the battle against attackers. Throughout this course section students will learn how SOC information management tools fit together, including incident management systems, threat intelligence platforms, SIEMs, and SOAR tools. We end the section describing the various groups of attackers, how their methods differ, and their motivations.

Topics: Introduction to the Blue Team Mission; SOC Overview; Defensible Network Concepts; Events, Alerts, Anomalies, and Incidents; Incident Management Systems; Threat Intelligence Platforms; SIEM; Automation and Orchestration; Who Are Your Enemies?

SECTION 2: Understanding Your Network

Section 2 begins the technical journey of understanding the environment. To defend a network, you must thoroughly understand its architecture and the impact that it will have on analysis. This section introduces the concepts of a modern organization's network traffic flow by dissecting a basic home Internet connection and describing the features necessary for segmentation and monitoring. These modules ensure that students have a firm grasp on how network design affects their "view of the world" as an analyst. We then go in-depth on common network services. Section 2 provides thorough working explanations of the current and upcoming features of DNS, HTTP(S), SMTP, and more, with a focus on the most important points for analysts to understand. These sections explain what normal data look like, as well as the common fields and areas that are used to spot anomalous behavior. The focus will be on quickly recognizing the common tricks used by attackers to turn these everyday services against us.

Topics: Corporate Network Architecture; Traffic Capture and Analysis; Understanding DNS; DNS Analysis and Attacks; Understanding HTTP and HTTPS; Analyzing HTTP for Suspicious Activity; How SMTP and Email Attacks Work; Additional Important Protocols

SECTION 3: Understanding Endpoints, Logs, and Files

It is extremely difficult to succeed at cyber defense without knowing where and how your data is produced, so Section 3 takes us down to the host, logging, and file level. Starting with a survey of common endpoint-based attack tactics, we orient students to the array of techniques that are used against their hosts. These first sections, followed by a section on defense in-depth, will give students an idea of how each step of the attack lifecycle aligns with its defensive tools, and what students can use to prevent and detect adversary attack advancement on their endpoints. To further prepare students for attack detection, these sections are followed by a thorough review of how Linux and Windows logging works. Reviewing logging capabilities gives students perspective on which logs will be present on any given system, where to find them, and how to interpret them. We cover several high-importance log events and provide an in-depth explanation of how to interpret Windows Kerberos logs. The course section then turns to the parsing and enrichment of logs, as well as how the SIEM normalization and categorization processes work. These topics give a complete view of what happens from the moment a log is generated to when it shows up in our security tools. Many new analysts struggle to understand how files are structured at a low level and therefore are hesitant when it comes to answering questions such as "could a file of type x be used for evil?" The final part of section 3 provides students with the concepts needed to reason through the answer, diving into files at the byte level. We explain the difference between binary and text-based files, and what makes a file a valid document, pdf, .exe, or something else. We also explain file-based exploitation methods and the features and formats most commonly seen in attacks. Concepts such as using strings, hashes, and file signatures are explained to show students how to quickly and accurately identify potentially malicious file samples. Students will finish this section understanding how different common file formats work, how they are typically weaponized, and how to quickly decide whether or not a given sample is likely to be malicious.

Topics: Endpoint Attack Tactics; Endpoint Defense In-Depth; How Windows Logging Works; How Linux Logging Works; Interpreting Important Events; Log Collection, Parsing, and Normalization; Files Contents and Identification; Identifying and Handling Suspicious Files

SECTION 4: Triage and Analysis

Now that the course has covered the ground required to understand the tools and data most frequently encountered by analysts, it's time to focus on analysis itself. This section will focus on how the analysis process works and explain how to avoid the common mistakes new analysts can slip into. We can combat the tendency to overlook the obvious by examining how our memory perception affects analysis and how cognitive biases cause us to fail to see what is right in front of us. The goal is to teach students not only how to think clearly, but also how to explain and leave a trail of how they reached their conclusions that can support future analysis and act as an audit trail. In addition to analysis technique, this course section covers both offensive and defensive mental models that are necessary to understand to perform high-quality analysis. Students will use these models to look at an alert queue and get a quick and intuitive understanding of which alerts may pose the biggest threat and which must be attended to first. Afterward, safe analysis techniques and analysis operational security concerns are discussed to ensure that analysts do not tip their hand to attackers during the investigation process. The section finishes discussing both how to react to identified intrusions and considerations for doing so as well as how to ensure high-quality documentation for incidents is produced and maintained. The goal is for students to leave this day better prepared to understand their alert queues, perform error-free investigation, and be able to choose the best response for any given attack situation.

Topics: Alert Triage and Prioritization; Perception and Investigation; Memory and Investigation; Mental Models for Information Security; Structured Analysis Techniques; Analysis Questions and Tactics; Analysis OPSEC; Intrusion Discovery; Incident Closing and Quality Review

SECTION 5: Continuous Improvement, Analytics, and Automation

Repetitive tasks, lack of empowerment or challenges, poorly designed manual processes – analysts know these pains all too well. While these are just some of the common experiences in day-to-day work, they are major contributing factors to unhappiness and burnout that can cause turnover in a SOC. Do things have to be this way? Of course not, but it will take some understanding and work on your part to do things differently. This section focuses squarely on improving the efficiency and enthusiasm of working in SOCs by tackling the most common problems head on. Through process optimization, careful analytic design and tuning, and workflow efficiency improvements, we can eliminate many of these common pain points. This frees us from the repetitive work we loathe and allows us to focus on what we do best – analysis! Having the time for challenging and novel work leads to a virtuous cycle of growth and engagement throughout the SOC – and improving everyone's life in the process. This section will focus on tuning your tools using clever analysis techniques and process automation to remove the monotonous and non-value-added activities from your day. We also cover containment activities, including the tools you can use and how to decide how to halt a developing incident or infection from the host or network angle. We'll wrap up the section with recommendations on skill growth, long-term career development, and how to get more involved in the cyber defense community.

Topics: Improving Life in the SOC; Analytic Features and Enrichment; New Analytic Design, Testing, and Sharing; Tuning and False Positive Reduction; Automation and Orchestration; Improving Operational Efficiency and Workflow; Containing Identified Intrusions; Skill and Career Development

SECTION 6: Capstone: Defend the Flag

The course culminates in a section-long, team-based capture-the-flag competition. Using network data and logs from a simulated network under attack, this final course section provides a full slate of hands-on work applying the principles taught throughout the course. Your team will be challenged to detect and identify attacks to progress through multiple categories of questions designed to ensure mastery of the concepts and data covered during the course.

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Security West	May 10
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

GOSI
Open Source Intelligence
giac.org/gosi

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Create an OSINT process
- Conduct OSINT investigations in support of a wide range of customers
- Understand the data collection life cycle
- Create a secure platform for data collection
- Analyze customer collection requirements
- Capture and record data
- Create sock puppet accounts
- Create your own OSINT process
- Harvest web data
- Perform searches for people
- Access social media data
- Assess a remote location using online cameras and maps
- Examine geolocated social media
- Research businesses
- Use government-provided data
- Collect data from the dark web
- Leverage international sites and tools

> **"Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!"**
>
> — Dave Huffman, **Rockwell Automation**

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. While the course is an entry point for people wanting to learn about OSINT, the concepts and tools taught are far from basic. The goal is to provide the OSINT groundwork knowledge for students to be successful in their fields, whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Many people think using their favorite Internet search engine is enough to find the data they need and do not realize that most of the Internet is not indexed by search engines. SEC487 teaches students effective methods of finding these data. You will learn real-world skills and techniques that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amounts of information found on the Internet. Once you have the information, we'll show you how to ensure that it is corroborated, how to analyze what you've gathered, and how to make sure it is useful in your investigations.

You will learn OSINT by completing more than 20 hands-on exercises using the live Internet and dark web.

Course Author Statement

"I have always been intrigued by the types and amount of data that are available on the Internet. From researching the best restaurants in a foreign town to watching people via video cameras, it all fascinates me. As the Internet evolved, more high-quality, real-time resources became available and every day was like a holiday, with new and wondrous tools and sites coming online and freely accessible.

"At a certain point, I was no longer in awe of the great resources on the web and, instead, transitioned to being surprised that people would post images of themselves in illegal or compromising positions or that a user profile contained such explicit, detailed content. My wonder shifted to concern for these people. What I found was that, if you looked in the right places, you could find almost anything about a person, a network, or a company. Piecing together seemingly random pieces of data into meaningful stories became my passion and, ultimately, the reason for this course.

"I recognized that the barrier to performing excellent OSINT was not that there was no free data on the Internet. It was that there was too much data on the Internet. The challenge transitioned from 'how do I find something' to 'how do I find only what I need.' This course was born from this need to help others learn the tools and techniques to effectively gather and analyze OSINT data from the Internet."

— Micah Hoffman

SEC487: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Foundations of OSINT

We begin with the basics and answer the questions "what is OSINT" and "how do people use it." This first section of this course is about level-setting and ensuring that all students understand the background behind what we do in the OSINT field. We also establish the foundation for the rest of the course by learning how to document findings and set up an OSINT platform. The information taught in this section is a key component for the success of an OSINT analyst because without these concepts and processes in place, researchers can get themselves into serious trouble during assessments by inadvertently alerting their targets or improperly collecting data.

Topics: Course Introduction; Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting up an OSINT Platform; Effective Habits and Process; Leveraging Search Engines

SECTION 2: Gathering, Searching, and Analyzing OSINT

OSINT data collection begins in Section 2 after we get a glimpse of some of the fallacies that could influence our conclusions and recommendations. From this point in the class forward, we examine distinct categories of data and think about what it could mean for our investigations. Retrieving data from the Internet could mean using a web browser to view a page or, as we learn in this section, using command line tools, scripts, and helper applications.

Topics: Data Analysis Challenges; Harvesting Web Data; File Metadata Analysis; OSINT Frameworks; Basic Data: Addresses and Phone Numbers; Basic Data: Email Addresses; User Names; Avatars and Reverse Image Searches; Additional Public Data; Creating Sock Puppets

SECTION 3: Social Media, Geolocation, and Imagery

Section 3 kicks off by examining free and paid choices in people search engines and understanding how to use the data we receive from them. Some of these engines provide social media content in their results. This makes a terrific transition for us to move into social media data, geolocation, and eventually mapping and imagery.

Topics: People Search Engines; Exercise People Searching; Facebook Analysis; LinkedIn Data; Instagram; Twitter Data; Geolocation; Imagery and Maps

SECTION 4: Networks, Government, and Business

Section 4 focuses on many different but related OSINT issues. This is our blue team section, as we dive into OSINT for IP addresses, domain names, DNS, and Whois. We then move into how to use wireless network information for OSINT. We end the section with two huge modules on searching international government websites for OSINT data and supporting business processes with OSINT.

Topics: Whois; IP Addresses; DNS; Finding Online Devices; Wireless Networks; Recon Tool Suites and Frameworks; Researching Company/Government Data

SECTION 5: The Dark Web, Breach Data, and International Issues

The beginning of section five focuses on understanding and using three of the dark web networks. Students will learn why people use Freenet, I2P, and Tor. Each network is discussed at length so that students don't just know how and why to use it, but also gain an understanding of how those networks work. With the Tor network being such a big player in the dark web, the course spends extra time diving into its resources. After tackling the dark web, we examine how we can use breach data in our cases and to address international OSINT issues. We end the section by examining how to find and track vehicles of all sizes. The end of this section is a massive lab, the Solo Capture-the-Flag (CTF) Challenge that helps students put together all that they have learned up until now in the course. Through a semi-guided walk-through that touches on many of the concepts taught throughout the course, students complete a full OSINT assessment at their own speed. Setting aside time to work through our OSINT process in an organized manner reinforces key concepts and allows students to practice executing OSINT process, procedures, and techniques.

Topics: The Surface, Deep, and Dark Webs; The Dark Web; Freenet; I2P – Invisible Internet Project; Tor; Monitoring and Alerting; International Issues; Vehicle Searches

SECTION 6: Capstone: Capture (and Present) the Flag

The capstone for the course is a group event that brings together everything that students have learned throughout the course. This is not a "canned" Capture-the-Flag event where specific flags are planted and your team must find them. It is a competition where each team will collect specific OSINT data about certain targets. The output from this work will be turned in as a "deliverable" to the "client" (the instructor and fellow classmates). This multi-hour, hands-on event will reinforce what the students practiced in the Solo CTF in the previous section before and add the complexity of performing OSINT assessments under pressure and in a group.

Who Should Attend

- Cyber incident responders
- Digital Forensics and Incident Response (DFIR) analysts
- Penetration testers
- Social engineers
- Law enforcement personnel
- Intelligence personnel
- Recruiters
- Private investigators
- Insurance investigators
- Human resources personnel
- Researchers

> **"The application of OSINT is broad. This course provides opportunities to apply it to my day-to-day work."**
>
> — Timothy DeBlock, **Premise Health**

Live Online sans.org/live-online

EVENT	START DATE
CTI Summit	Jan 25
OSINT Summit	Feb 15
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Security West	May 10
Purple Team Summit	May 17
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC501: **Advanced Security Essentials – Enterprise Defender**

GCED
Enterprise Defender
giac.org/gced

6 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Access tools that can be used to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process
- Use various tools to identify and remediate malware across your organization
- Create a data classification program and deploy data loss prevention solutions at both a host and network level

> **"SEC501 is a very valuable course to a Network/Security Administrator. The first chapter of Defensible Network Architecture is worth the price of admission in and of itself."**
>
> — Ryan Bast, **Subzero Group, Inc.**

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Course Author Statement

"I started off working as a network engineer and architect building enterprise networks. This role organically transitioned into secure design and engineering. My interest at the time in penetration testing and exploitation allowed me to verify that our designs being put into production were truly hardened. This interest eventually drove me into a career in full-blown reverse engineering and 0-day bug discovery/exploit development. After a long history of writing and teaching courses for SANS on advanced penetration testing and exploit writing, I am excited to take that experience and apply it back into defense. We selected a group of rock star authors to build the SEC501 syllabus and content, including Dave Shackleford, Phil Hagen, Matt Bromiley, and Rob Vandenbrink."
— Stephen Sims

SEC501: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Defensive Network Architecture

Section 1 will focus on security in the design and configuration of various enterprise infrastructures. From a security perspective, proper design and configuration protects both the components being configured, as well as the rest of the organization that depends on that gear to defend other components from attacks. In other words, a good house needs a good foundation! We'll discuss published security benchmarks, vendor guidance for securing various products, and regulatory requirements and how they impact defending infrastructure against specific attacks. To illustrate these points, we'll be looking in detail at securing and defending a router infrastructure against a number of device- and network-based attacks. In addition, we'll cover securing Windows and Active Directory against specific attacks. Securing private and public cloud Infrastructure against common attacks will also be discussed, and Active Defense approaches will be covered in some detail.

Topics: Security Benchmarks, Standards, and the Role of Audit in Defending Infrastructure; Defense Using Authentication and Authorization, and Defending Those Services; The Use of Logging and Security Information and Event Management (SIEM) in Defending an Organization from Attack; Attacking and Defending Critical Protocols; Several Man-in-the-Middle Attack Methods, and Defenses against Each; Infrastructure Defense Using IPS, Next-Generation Firewalls, and Web Application Firewalls; Defense of Critical Servers and Services; Active Defense; Defense of Private and Public Cloud Architectures

SECTION 2: Penetration Testing

Security is all about understanding, mitigating, and controlling the risk to an organization's critical assets. An organization must understand the changing threat landscape and have the capacity to compare it against its own vulnerabilities that could be exploited to compromise the environment. In Section 2, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration tests to better understand the security posture for network services, operating systems, and applications. In addition, we'll talk about social engineering and reconnaissance activities to better emulate increasingly prevalent threats to users.

Topics: Introduction to Penetration Testing Concepts; Penetration Testing Scoping and Rules of Engagement; Online Reconnaissance and Offensive Counterintelligence; Social Engineering; Network Mapping and Scanning Techniques; Enterprise Vulnerability Scanning; Network Exploitation Tools and Techniques; Web Application Exploitation Tools and Techniques; Post-Exploitation and Pivoting; OS and Application Exploit Mitigations; Reporting and Debriefing

SECTION 3: Security Operations Foundations

Traffic analysis and intrusion detection used to be treated as a separate discipline within many organizations. Today, prevention, detection, and response must be closely knit, so that once an attack is detected, defensive measures can be adapted and proactive forensics implemented, and the organization can to continue to operate. This course section will start with a brief introduction to network security monitoring, followed by a refresher on network protocols with an emphasis on fields to look for as security professionals. We'll use tools like TCPdump and Wireshark to analyze packet traces and look for indicators of attacks. We'll use a variety of detection and analysis tools, craft packets with Scapy to test detection, and touch on network forensics and the Security Onion monitoring distribution. Students will also explore Snort as a network Intrusion Detection System, and examine rule signatures in-depth.

Topics: Network Security Monitoring; IP, TCP, and UDP Refresher; Advanced Packet Analysis; Introduction to Network Forensics with Security Onion; Identifying Malicious Content and Streams; Extracting and Repairing Content from PCAP files; Traffic Visualization Tools; Intrusion Detection and Intrusion Prevention; Handling Encrypted Network Traffic

SECTION 4: Digital Forensics and Incident Response

In this section, you will learn the core concepts of both "Digital Forensics" and "Incident Response." We'll explore some of the hundreds of artifacts that can give forensic investigators specific insight about what occurred during an incident. You will also learn how incident response currently operates, after years of evolving, in order to address the dynamic procedures used by attackers to conduct their operations. We'll look at how to integrate DFIR practices into a continuous security operations program. We'll cover the general guidelines for a cyclical, six-step incident response process. Each step will be examined in detail, including practical examples of how to apply it. Lastly, you'll learn the artifacts that can best be used to determine the extent of suspicious activity within a given environment and how to migrate techniques to a large data set for enterprise-level analysis.

Topics: DFIR Core Concepts: Digital Forensics; DFIR Core Concepts: Incident Response; Modern DFIR: A Live and Continuous Process; Widening the Net: Scaling the DFIR Process and Scoping a Compromise

SECTION 5: Malware Analysis

Malicious software is responsible for many incidents in almost every type of organization. Types of malware vary widely, from Ransomware and Rootkits to Crypto Currency Miners and worms. We will define each of the most popular types of malware and walk through multiple examples. The four primary phases of malware analysis will be covered: Fully Automated Analysis, Static Properties Analysis, Interactive Behavior Analysis, and Manual Code Reversing. You will complete various in-depth labs requiring you to fully dissect a live Ransomware specimen from static analysis through code analysis. You will get hands-on experience with tricking the malware through behavioral analysis techniques, as well as decrypting files encrypted by Ransomware by extracting the keys through reverse engineering. All steps are well defined and tested to ensure that the process to achieve these goals is actionable and digestible.

Topics: Introduction to Malware Analysis; The Many Types of Malware; ATM/Cash Machine Malware; Building a Lab Environment for Malware Analysis; Malware Locations and Footprints; Fully Automated Malware; Cuckoo Sandbox; Static Properties Analysis; Interactive Behavior Analysis; Manual Code Reversing; Tools such as IDA, PeStudio, ILSpy, Process Hacker, Process Monitor, NoFuserEx, etc.

SECTION 6: Enterprise Defender Capstone

The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, use the skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they submit flags to score points. More difficult challenges will be worth more points. In this defensive exercise, challenges include packet analysis, routing protocols, scanning, malware analysis, and other challenges related to the course material.

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Scottsdale: Virtual Edition	Feb 22
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Rocky Mountain Spring	Apr 26
Security West	May 10
Cyber Security Central: June	Jun 7

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! SEC503: **Intrusion Detection In-Depth**

GCIA
Intrusion Analyst
giac.org/gcia

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

SEC503 is one of the most important courses that you will take in your information security career. While past students describe it as the most difficult class they have ever taken, they also tell us it was the most rewarding. This course isn't for people who are simply looking to understand alerts generated by an out-of-the-box Intrusion Detection System (IDS). It's for people who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about. If you want to be able to find zero-day activities on your network before disclosure, this is definitely the class for you.

What sets this course apart from any other training is that we take a bottom-up approach to teaching network intrusion detection and network forensics. Rather than starting with a tool and teaching you how to use that tool in different situations, this course teaches you how and why TCP/IP protocols work the way they do. After spending the first two course sections examining what we call "Packets as a Second Language," we add in common application protocols and a general approach to researching and understanding new protocols. With this deep understanding of how network protocols work, we turn our attention to the most widely used tools in the industry to apply this deep knowledge. The result is that you will leave this class with a clear understanding of how to instrument your network and the ability to perform detailed incident analysis and reconstruction.

These benefits alone make this training completely worthwhile. What makes the course as important as we believe it is (and students tell us it is), is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today.

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic, and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

This course delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master a variety of tools, including tcpdump, Wireshark, Snort, Zeek, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Evening Bootcamp sessions and exercises force you to take the theory taught during the section and apply it to real-world problems immediately. Basic exercises include assistive hints, while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

A Virtual machine (VM) is provided with tools of the trade. It is supplemented with demonstration PCAPs containing network traffic. This allows you to follow along on your laptop with the course material and demonstrations. The PCAPs also provide a good library of network traffic to use when reviewing the material, especially for the GCIA certification associated with this course.

> **"SEC503 completely changed how I look at networking and how I approach problems, and it significantly increased my understanding of intrusion detection."**
>
> — Arnold Klein, **Topel Forman Information Services, LLC**

SEC503: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Fundamentals of Traffic Analysis: Part 1

The first section of this course begins our bottom-up coverage of the TCP/IP protocol stack, providing a refresher or introduction, depending on your background, to TCP/IP. This is the first step in what we think of as a "Packets as a Second Language" course. Students begin to be introduced to the importance of collecting the actual packets involved in attacks and are immediately immersed in low-level packet analysis. We will cover the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, and the meaning and expected behavior of every field in the IP header. Students are introduced to the use of open-source Wireshark and tcpdump tools for traffic analysis.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

SECTION 3: Signature-Based Detection

Section 3 builds on the foundation of the first two sections of the course, moving into the world of application layer protocols. Students are introduced to the versatile packet crafting tool Scapy. This is a very powerful Python-based tool that allows for the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. Various practical scenarios and uses for Scapy are provided throughout this section.

Topics: Scapy; Advanced Wireshark; Detection Methods for Application Protocols; DNS; Microsoft Protocols; HTTP(2)/TLS; SMTP; IDS/IPS Evasion Theory; Identifying Traffic of Interest

SECTION 5: Modern and Future Monitoring: Forensics, Analytics, and Machine Learning

Section 5 continues the trend of less formal instruction and more practical application in hands-on exercises. It consists of three major topics, beginning with practical network forensics and an exploration of data-driven monitoring vs. alert-driven monitoring, followed by a hands-on scenario that requires students to use all of the skills developed so far. The second topic continues the theme of data-driven analysis by introducing large-scale analysis and collection using NetFlow and IPFIX data. Following a discussion of the powerful correlations and conclusions that can be drawn using the network metadata, students will work on a second guided scenario that leverages this set of tools, in addition to other skills learned throughout the week. The section concludes with a detailed discussion of practical TLS analysis and interception and more general command and control trends and detection/analysis approaches. A third scenario is provided for students to work on after class.

Topics: Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

SECTION 2: Fundamentals of Traffic Analysis: Part 2

Section 2 continues where the first section ended, completing the "Packets as a Second Language" portion of the course and laying the foundation for the much deeper discussions to come. In this section, students will gain a deep understanding of the primary transport layer protocols used in the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using advanced features to give you the skills to analyze your own traffic. The focus of these tools is to filter large scale data down to traffic of interest using Wireshark display filters and tcpdump Berkeley Packet Filters. These are used in the context of our exploration of the TCP/IP transport layers covering TCP, UDP, and ICMP. Once again, we discuss the meaning and expected function of every header field, covering a number of modern innovations that have very serious implications for modern network monitoring, and we analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Wireshark Display Filters; Writing BPF Filters; TCP; UDP; ICMP; Real-World Analysis – Command Line Tools

SECTION 4: Anomalies and Behaviors

The fundamental knowledge gained from the first three sections provides the foundation for deep discussions of modern network intrusion detection systems during Section 4. Everything that students have learned so far is now synthesized and applied to designing optimized detection rules for Snort/Firepower, and this is extended even further with behavioral detection using Zeek (formerly known as Bro).

Topics: Network Architecture; Introduction to IDS/IPS Analysis; Snort; Zeek

SECTION 6: IDS Capstone Challenge

The course culminates with a fun, hands-on, score-server-based IDS challenge. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the first five sections. The challenge presented is based on hours of live-fire, real-world data in the context of a time-sensitive incident investigation. The challenge is designed as a "ride-along" event, where students are answering questions based on the analysis that a team of professional analysts performed of this same data.

Who Should Attend

- Intrusion detection (all levels), system, and security analysts
  - Analysts will be introduced to or become more proficient in the use of traffic analysis tools for signs of intrusions.
- Network engineers/administrators
  - Network engineers/administrators will understand the importance of optimal placement of IDS sensors and how the use of network forensics such as log data and network flow data can enhance the capability to identify intrusions.
- Hands-on security managers
  - Hands-on security managers will understand the complexities of intrusion detection and assist analysts by providing them with the resources necessary for success.

> **"I have a deeper understanding of the topics from my class. This will help me get more data out of my investigations."**
>
> — Alphonse Wichrowski, **Allegiant Air**

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
Cyber Security West: Feb	Feb 1
Cyber Security East: March	Mar 1
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Baltimore Spring: Virtual Edition	Apr 26
Security West	May 10
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC505: **Securing Windows and PowerShell Automation**

GCWN
Windows Security Administrator
giac.org/gcwn

6
Day Program

36
CPEs

Laptop
Required

You Will Be Able To

- Write PowerShell scripts for security automation
- Execute PowerShell scripts on remote systems
- Harden PowerShell itself against abuse, and enable transcription logging for your SIEM
- Use PowerShell to access the WMI service for remote command execution, searching event logs, reconnaissance, and more
- Use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds (assume breach)
- Block the lateral movement of hackers and ransomware using Windows Firewall, IPsec, DNS sinkholes, admin credential protections, and more
- Prevent exploitation using AppLocker and other Windows OS hardening techniques in a scalable way with PowerShell
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root
- Configure mitigations against pass-the-hash attacks, Kerberos Golden Tickets, Remote Desktop Protocol (RDP) man-in-the-middle attacks, Security Access Token abuse, and other attacks discussed in SEC504 and other SANS hacking courses
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certificate Authentications (CAs)
- Harden essential protocols against exploitation, such as SSL, RDP, DNS, PowerShell Remoting, and SMB

> **"SEC505 is the gold standard of Windows security training."**
>
> — Alexander Kotkov, **EY**

WINDOWS SECURITY AUTOMATION MEANS POWERSHELL

In this course you will learn how to:

- Write PowerShell scripts for Windows and Active Directory security automation
- Safely run PowerShell scripts on thousands of hosts over the network
- Defend against PowerShell malware such as ransomware
- Harden Windows Server and Windows 10 against skilled attackers

In particular, we will use PowerShell to secure Windows against many of the attacks described in the MITRE ATT&CK matrix, especially stolen administrative credentials, ransomware, hacker lateral movement inside the LAN, and insecure Windows protocols, like RDP and SMB.

You will leave this course ready to start writing your own PowerShell scripts to help secure your Windows environment. It's easy to find Windows security checklists, but how do you automate those changes across thousands of machines? How do you safely run scripts on many remote boxes? In this course you will learn not just Windows and Active Directory security, but how to manage security using PowerShell.

DON'T JUST LEARN POWERSHELL SYNTAX, LEARN HOW TO LEVERAGE POWERSHELL AS A FORCE MULTIPLIER FOR WINDOWS SECURITY

There is another reason why PowerShell has become popular: PowerShell is just plain fun! You will be surprised at how much you can accomplish with PowerShell in a short period of time – it's much more than just a scripting language, and you don't have to be a coding guru to get going.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for IT people with PowerShell skills. You don't have to know any PowerShell to attend this course, we will learn it together during the labs.

You can learn basic PowerShell syntax on YouTube for free, but this course goes far beyond syntax. In this course we will learn how to use PowerShell as a platform for managing security, as a "force multiplier" for the Blue Team, and as a rocket booster for your Windows IT career.

WE WILL WRITE A POWERSHELL RANSOMWARE SCRIPT AND DEFEND AGAINST IT

Unfortunately, PowerShell is being abused by hackers and malware authors, so in the last section of the course, we will write our own ransomware script to see how to defend against scripts like it.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security at the same time.

The course author, Jason Fossen, is a SANS Institute Fellow and has been writing and teaching for SANS since 1998. In fact, SEC505 has had at least one day of PowerShell for more than 10 years, and now PowerShell is the centerpiece of the course.

◀ RETURN TO TABLE OF CONTENTS

SEC505: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Learn PowerShell Scripting for Security

This course section covers what you need to know to get started using PowerShell. You do not need to have any prior scripting or programming experience. We have PowerShell labs throughout the course, so this section is not the only PowerShell material. We start with the essentials, then go more in depth as the course progresses. Do not worry, you will not be left behind, the PowerShell labs walk you through every step. If you already have PowerShell experience, then there will be intermediate topics for you too.

Topics: PowerShell IS Dangerous (and Fun); Writing Your Own Scripts, Functions, and Modules; Up and Running Quickly with PowerShell; Piping Objects Instead of Text

SECTION 2: You Don't Know the POWER!

How can we run PowerShell scripts on thousands of systems with just a few lines of code? This section is about remote command execution using PowerShell Remoting, the SSH service on Windows, the Task Scheduler service, and boot up scripts assigned through Group Policy.

Topics: PowerShell Remoting; OpenSSH on Windows; PowerShell Just Enough Admin (JEA); PowerShell, Group Policy, and the Task Scheduler

SECTION 3: WMI and Active Directory Scripting

PowerShell is deeply integrated into the Windows Management Instrumentation (WMI) service. Many PowerShell commands are just wrappers for WMI functions. Hackers love the WMI service too, but for the wrong reasons. The WMI service is enabled by default and accessible over the network. With our PowerShell WMI scripts we can remotely execute commands, reboot machines, forcibly log users off, kill processes, and much more. Today, we will see how to do all this. WMI scripting is a bit difficult, but we'll go through all the strange namespaces and classes together. In this section we will also use PowerShell to search, manage, and secure Active Directory. With PowerShell we can find abandoned user accounts and disable them. We can enforce our desired group memberships with scheduled scripts. We can reset passwords on thousands of user accounts. And when hackers are brute-forcing passwords, our PowerShell scripts can find the accounts being targeted. Of course, malicious insiders can do much of the same, such as with the Bloodhound tool, so we'll examine how we can restrict what users can see or change.

Topics: PowerShell for WMI; PowerShell for Active Directory; Active Directory Permissions and Auditing

SECTION 4: Hardening Network Services with PowerShell

In this course section, we will use PowerShell and Group Policy to automate the hardening of many exploitable services and protocols, such as Kerberos, Domain Name System (DNS), Remote Desktop Protocol (RDP), and File and Printer Sharing (SMB). Think of Kerberos Golden Tickets, DNS response spoofing, the Bluekeep RDP attack, the EternalBlue/WannaCry SMB worm, and other attacks

Topics: Server Hardening Automation for DevOps; Windows Firewall Scripting; Share Permissions for TCP/UDP Listening Ports with IPsec; Exploitable Protocols and Services

SECTION 5: Certificates and Multifactor Authentication

Smart cards and smart tokens, such as YubiKeys, are the gold standard for multi-factor authentication (MFA). In this course section, we will use PowerShell to install a certificate server that can be used to deploy smart cards and smart USB tokens. Smart cards and tokens can be used for PowerShell Remoting, signing PowerShell scripts, Remote Desktop Protocol (RDP) logons, User Account Control (UAC), ASP.NET web application logons, and more.

Topics: Certificate Authentication and TLS Encryption for PowerShell; Installing a Windows Certificate Server with PowerShell; Deploying Smart Cards, Smart Tokens, and TPM Virtual Smart Cards; Security Best Practices

SECTION 6: PowerShell Security, Ransomware, and DevOps

In this course section, we will write a PowerShell ransomware script and unleash it inside our training VM (don't release it into the wild, you'll go to federal prison). The purpose of this ethical hacking is to discuss defenses against this kind of PowerShell abuse. How can we secure PowerShell itself? PowerShell is not a single tool. There is no one registry value or patch to magically make PowerShell "secure," but there is a lot we can do. In this section we will cover many defensive techniques to prevent future compromises, reduce the harm we suffer after a compromise, and gain visibility into PowerShell malicious activity for the sake of forensics, incident response, and threat hunting.

Topics: PowerShell Ransomware; Anti-Exploitation Defenses for PowerShell; PowerShell Visibility AND Detection; Capstone: DevOps Automation with PowerShell

Who Should Attend

- Anyone who wants to learn PowerShell automation
- Defenders on the Blue Team
- Windows endpoint and server administrators
- Anyone implementing the CIS Critical Security Controls
- Anyone implementing the MITRE ATT&CK mitigations

> **"This class provided real-world examples and sample scripts to make a Windows-centric environment fundamentally more secure."**
>
> — Nick Boardman, **HRSD**

Live Online **sans.org/live-online**

EVENT	START DATE
Cyber Security West: Feb	Feb 1
SANS 2021	Mar 22
Security West	May 10
Cyber Security Central: June	Jun 7

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC511: **Continuous Monitoring and Security Operations**

GMON
Continuous Monitoring
giac.org/gmon

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centers (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP 800-137

> **"SEC511 was a wonderful look into the world of the 'Blue Team.' The authors really put together a robust course full of great ideas and tactics to take on intrusion detection and continuous monitoring."**
>
> — Cameron Johns, **Tyson Foods, Inc.**

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. SEC511 will teach you how to strengthen your skills to undertake that proactive approach.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and section five of this course will greatly increase your understanding and enhance your skills in implementing CM using the NIST framework.

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification, and both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final section features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. The competition has been designed to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

With your training journey now complete and your skills enhanced and honed, it is time to go back to work and deliver on the SANS promise that you will be able to apply what you learn in this course the day you return to the office.

> **"SEC511 is a VERY worthwhile addition to the Cyber Defense curriculum for Blue Teamers."**
>
> — Robert Peden, **NextGear Capital**

SEC511: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Current State Assessment, Security Operations Centers, and Security Architecture

The prevention-dominant security model has failed. Given the frequency and extent of significant intrusions, this should not come as a surprise. In order to address the root of the problem, we must understand the current architecture and the design gaps that facilitate the adversary's dominance. What do we need to address to begin to make things better? Can we ever hope to win? What would winning look like? These are important questions that we must answer if we hope to substantially improve our security posture. We begin with the end in mind, and define the key techniques and principles that will allow us to achieve that state. An effective modern Security Operations Center or security architecture must enable an organization's ability to rapidly find intrusions to facilitate containment and response. Both significant knowledge and a commitment to continuous monitoring are required to achieve this goal.

Topics: Overview; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture - Key Techniques/Practices; Security Operations Center (SOC)

SECTION 2: Network Security Architecture

Understanding the problems with the current environment and realizing where we need to get to is far from sufficient: we need a detailed roadmap to bridge the gap between the current and desired state. Section 2 introduces and details the components of our infrastructure that become part of a defensible network security architecture and SOC. We are long past the days when a perimeter firewall and ubiquitous antivirus were sufficient security. There are many pieces and moving parts that make up a modern defensible security architecture. In addition to discussing technologies like Next Generation Firewalls, UTM devices, Malware Detonation Devices, SIMs, DLP, and Honeypots that may not be found in all organizations, we will focus on repurposing traditional devices such as layer 3/4 firewalls, routers, switches, and NIDS. The goal of this course is not to give you a long list of items to add to the next year's budget, so we will focus on maximizing the capabilities of your current information security architecture, while pointing out new technologies that may offer a compelling return on investment.

Topics: SOCs/Security Architecture - Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

SECTION 3: Network Security Monitoring

Designing a SOC or security architecture that enhances visibility and detective capabilities represents a paradigm shift for most organizations. However, the design is simply the beginning. The most important element of a modern security architecture is the emphasis on detection. The network security architecture presented in sections one and two emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise. We must first understand the approach and goals of monitoring and define a methodology for analysis. Key terms such as Network Security Monitoring (NSM), Continuous Diagnostics and Mitigation (CDM), and Continuous Security Monitoring (CSM) can cause confusion, and we will make sure these terms are understood, enabling the security professional to guide an organization in using the best practices. Speaking of best practices, we will emphasize the continuous monitoring of the Critical Security Controls. Enabling continuous monitoring will be studied by developing a model for employing robust NSM. This will allow an organization to deal with and make sense of data to rapidly enable the detection of potential intrusions or unauthorized actions.

Topics: Continuous Monitoring Overview; Network Security Monitoring (NSM)

SECTION 4: Endpoint Security Architecture

One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Section 4 details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

Topics: Security Architecture – Endpoint Protection; Dangerous Endpoint Applications; Patching

SECTION 5: Automation and Continuous Security Monitoring

Network Security Monitoring (NSM) is the beginning; we need to not only detect active intrusions and unauthorized actions, but also to know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need to be addressed. The volume of data that must be continuously sought and mined is vast: the goal of continuous monitoring would be out of reach without scripting and automation. Naturally, there are vendors and tools to scratch this itch, but they will be incomplete and require their own care, feeding, and monitoring. Section 5 describes how to perform continuous monitoring with simple tools and scripts. Knowing how to script and automate is pointless unless you know what data should be captured and analyzed on a continuous basis. Again leaning on the Critical Security Controls, we will determine high-value targets for continuous monitoring in an enterprise.

Topics: Overview; Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation

SECTION 6: Capstone: Design, Detect, Defend

The course culminates in a team-based Design, Detect, and Defend-the-Flag competition that is a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques you have been learning during the course. From security architecture, network security monitoring, endpoint security, and continuous monitoring, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

Topics: Security Architecture; Assessing Provided Architecture; Continuous Security Monitoring; Using Tools/Scripts Assessing the Initial State; Quickly/Thoroughly Finding All Changes Made

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
Cyber Security East: March	Mar 1
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Security West	May 10
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC530: **Defensible Security Architecture and Engineering**

GDSA
Defensible Security Architecture
giac.org/gdsa

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Implement technologies for enhanced prevention, detection, and response capabilities
- Comprehend deficiencies in security solutions and understand how to tune and operate them
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

> **"This training showed how the overall security posture of an organization can be improved. It helps connect the dots between different areas within security infrastructure."**
>
> — Farruk Ali, **UPS**

SEC530: Defensible Security Architecture and Engineering is designed to help students establish and maintain a holistic and layered approach to security. Effective security requires a balance between detection, prevention, and response capabilities, but such a balance demands that controls be implemented on the network, directly on endpoints, and within cloud environments. The strengths and weaknesses of one solution complement another solution through strategic placement, implementation, and fine-tuning.

To address these issues, this course focuses on combining strategic concepts of infrastructure and tool placement while also diving into their technical application. We will discuss and identify what solutions are available and how to apply them successfully. Most importantly, we'll evaluate the strengths and weaknesses of various solutions and how to layer them cohesively to achieve defense-in-depth.

The changing threat landscape requires a change in mindset, as well as a repurposing of many devices. Where does this leave our classic perimeter devices such as firewalls? What are the ramifications of the "encrypt everything" mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture and how to engineer it. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to significantly improve their organizations' prevention capabilities in the face of today's dynamic threat landscape. The course will also delve into the latest technologies and their capabilities, strengths, and weaknesses. You will come away with recommendations and suggestions that will aid in building a robust security infrastructure.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Multiple hands-on labs conducted daily will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

NOTE: The term "architecture" is interpreted differently by different organizations and in various regions of the world. This course focuses on strategic and technical application and use cases, including fine-tuning and implementing various infrastructure components and cyber defense techniques. If you are expecting the course to focus exclusively on strategic solution placement and use cases, the course is not for you.

> **"Every day of SEC530 has provided new insight and information. The labs are great, and I can't wait to put it all together. No matter how experienced a professional you are, SANS always teaches you something new."**
>
> — Ron Foupht, **Sirius Computer Solutions**

SEC530: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Defensible Security Architecture and Engineering

This first section of the course describes hardening systems and networks, beginning with the overall network architecture and layers. To quote Richard Bejtlich's *The Tao of Network Security Monitoring*, defensible networks "encourage, rather than frustrate, digital self-defense." The section begins with an overview of traditional network and security architectures and their common weaknesses. The defensible security mindset is "build it once, build it right." All networks must perform their operational functions effectively, and security can complement this goal. It is much more efficient to bake security in at the outset than to retrofit it later. The discussion will then turn to lower layer networking concepts, including many "ripped from the headlines" tips the co-authors have successfully deployed in the trenches to harden infrastructure in order to prevent and detect modern attacks. Examples include the use of private VLANs, which effectively kills the malicious client-to-client pivot, and 802.1X and NAC, which mitigate rogue devices. Specific Cisco IOS syntax examples are provided to harden switches.

Topics: Traditional Security Architecture Deficiencies; Defensible Security Architecture; Threat, Vulnerability, and Data Flow Analysis; Layer 1 Best Practices; Layer 2 Best Practices; NetFlow

SECTION 2: Network Security Architecture and Engineering

This section develops the discussion on hardening infrastructure and moves on to concepts such as routing devices, firewalls, and application proxies. Actionable examples are provided for hardening routers, with specific Cisco IOS commands to perform each step. The section then continues with a deep dive on IPv6, which currently accounts for 23 percent of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. We will provide deep background on IPv6, discuss common mistakes (such as applying an IPv4 mindset to IPv6), and provide actionable solutions for securing the protocol. The section wraps up with a discussion on firewalls and application proxies.

Topics: Layer 3: Router Best Practices; Layer 3 Attacks and Mitigation; Layer 2 and 3 Benchmarks and Auditing Tools; Securing SNMP; Securing NTP; Bogon Filtering, Blackholes, and Darknets; IPv6; Securing IPv6; VPN; Layer 3/4 Stateful Firewalls; Proxy

SECTION 3: Network-Centric Security

Organizations own or have access to many network-based security technologies, ranging from Next-Generation Firewalls to web proxies and malware sandboxes. Yet the effectiveness of these technologies is directly affected by their implementation. Too much reliance on built-in capabilities like application control, antivirus, intrusion prevention, data loss prevention, or other automatic evil-finding deep packet inspection engines leads to a highly preventative-focused implementation, with huge gaps in both prevention and detection. This section focuses on using application-layer security solutions that an organization already owns with a modern mindset. By thinking outside the box, even old controls like a spam appliance can be used to catch modern attacks such as phishing via cousin domains and other spoofing techniques. And again, by engineering defenses for modern attacks, both prevention and detection capabilities gain significantly.

Topics: NGFW; NIDS/NIPS; Network Security Monitoring; Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service

SECTION 4: Data-Centric Security

Organizations cannot protect something they do not know exists. The problem is that critical and sensitive data exist all over. Complicating this even more is that data are often controlled by a full application stack involving multiple services that may be hosted on-premise or in the cloud. This section focuses on identifying core data where they reside and how to protect those data. Protection includes using data governance solutions and full application stack security measures such as web application firewalls and database activity monitoring, as well as keeping a sharp focus on securing the systems hosting core services such as on-premise hypervisors, cloud computing platforms, and container services such as Docker. The data-centric security approach focuses on what is core to an organization and prioritizes security controls around it. Why spend copious amounts of time and money securing everything when controls can be optimized and focused on securing what matters? Let's face it: Some systems are more critical than others.

Topics: Application (Reverse) Proxies; Full Stack Security Design; Web Application Firewalls; Database Firewalls/Database Activity Monitoring; File Classification; Data Loss Prevention (DLP); Data Governance; Mobile Device Management (MDM) and Mobile Application Management (MAM); Private Cloud Security; Public Cloud Security; Container Security

SECTION 5: Zero Trust Architecture: Addressing the Adversaries Already in Our Networks

Today, a common security mantra is "trust but verify." But this is a broken concept. Computers are capable of calculating trust on the fly, so rather than thinking in terms of "trust but verify" organizations should be implementing "verify then trust." By doing so, access can be constrained to appropriate levels at the same time that access can become more fluid. This section focuses on implementing a zero-trust architecture where trust is no longer implied but must be proven. By doing so, a model of variable trust can be used to change access levels dynamically. This, in turn, allows for implementing fewer or more security controls as necessary given a user's and a device's trust maintained over time. The focus is on implementing zero-trust architecture with existing security technologies to maximize their value and impact for an organization's security posture. During this section encryption and authentication will be used to create a hardened network, whether external or internal. Also, advanced defensive techniques will be implemented to stop modern attack tools in their tracks while leaving services fully functional for authorized assets.

Topics: Zero Trust Architecture; Credential Rotation; Compromised Internal Assets; Securing the Network; Tripwire and Red Herring Defenses; Patching; Deputizing Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis

SECTION 6: Hands-On Secure-the-Flag Challenge

The course culminates in a team-based Design-and-Secure-the-Flag competition. Powered by NetWars, Section 6 provides a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted throughout this course. Teams will assess, design, and secure a variety of computer systems and devices, leveraging all seven layers of the OSI model.

Topics: Capstone – Design/Detect/Defend

Who Should Attend

- Security architects
- Network engineers
- Network architects
- Security analysts
- Senior security engineers
- System administrators
- Technical security managers
- CND analysts
- Security monitoring specialists
- Cyber threat investigators

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
Cyber Security East: Feb	Feb 22
Cyber Security West: March	Mar 15
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Rocky Mountain Spring	Apr 26
Security West	May 10
Cyber Security East: May	May 17
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC555: **SIEM with Tactical Analytics**

GCDA
Detection Analyst
giac.org/gcda

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open-source solutions (e.g., SOF-ELK)
- Get up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them
- Use log data to establish security control effectiveness
- Implement log alerts that create virtual tripwires for early breach detection

Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of those sources for proper analysis. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. The class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a “Big Data” problem but rather a “Data Analysis” problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the “appropriate” use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, how to start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

> **“This course uses real-world events and hands-on training to allow me to immediately improve my organization’s security stance. Day 1 back in the office, I was implementing what I learned.”**
>
> — Frank Giachino, **Bechtel Corp.**

SEC555: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: SIEM Architecture

Logging and analysis is a critical component in cyber network defense and allows for both reactive and proactive detection of adversarial activities. When properly utilized it becomes the backbone for agile detection and provides understanding to the overall environment. Logging and analysis products and techniques have been around for many years and are quickly gaining more and more functionality. This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to deal with the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Section 1 is designed to bring all students up to speed on SIEM concepts and bring them to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During this first course section, we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK (a VM co-maintained by Phil Hagen and Justin Henderson) and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

Topics: State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting

SECTION 2: Service Profiling with SIEM

A vast majority of network communication occurs over key network protocols and yet it is uncommon for organizations to use or collect this data. The sheer volume can be overwhelming. However, these common data sources provide an opportunity in identifying modern day attacks. This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered as well as passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as it is collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

Topics: Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Applying Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations

SECTION 3: Advanced Endpoint Analytics

The value in endpoint logs provides tremendous visibility in detecting attacks. Especially, with regard to finding post-compromise activity, endpoint logs can quickly become a vehicle that is second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousand events per day. Multiply this by the number of systems in your environment and it is no surprise why organizations get overwhelmed. This section will cover the how and more importantly the why behind collecting system logs. Various collection strategies and tools will be used to gain hands-on experience and to provide simplification with handling and filtering the seemingly infinite amount of data generated by both servers and workstations. Workstations' log strategies will be covered in depth due to their value in today's modern attack vectors. After all, modern day attacks typically start and then spread from workstations.

Topics: Endpoint Logs

SECTION 4: Baselining and User Behavior Monitoring

Know thyself is often quoted to defenders as a key defense strategy. And yet this is one of the most difficult things to accomplish. Take something such as having a list of all assets in an organization and knowing if any non-company assets are on the network. The task sounds simple but ends up being incredibly difficult to maintain in today's ever-evolving networks. This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized vs. unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in applying network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.

Topics: Identifying Authorized and Unauthorized Assets; Identifying Authorized and Unauthorized Software; Baseline Data

SECTION 5: Tactical SIEM Detection and Post-Mortem Analysis

Multiple security devices exist but often are designed to be independent. Analysts are commonly divided into specialty areas and focus on their respective area such as a network intrusion detection system. However, alerts from a single security device lack context and are akin to the common analogy of "looking up from the bottom of a well." This section focuses on combining multiple security logs for central analysis. More importantly we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, compromise is just the beginning and not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires. Should a single one be "stepped on" we can quickly detect and respond to the adversary.

Topics: Centralizing NIDS and HIDS Alerts; Analyzing Endpoint Security Logs; Augmenting Intrusion Detection Alerts; Analyzing Vulnerability Information; Correlating Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitoring Firewall Activity; SIEM Tripwires; Post-Mortem Analysis

SECTION 6: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, This final course section provides a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted during the course. From building a logging architecture, augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to finding attacks, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

Topics: Defend-the-Flag Challenge – Hands-on Experience

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

Live Online sans.org/live-online

EVENT	START DATE
CTI Summit	Jan 25
Scottsdale: Virtual Edition	Feb 22
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Security West	May 10
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC573: **Automating Information Security with Python**

GPYC
Python Coder
giac.org/gpyc

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Customize existing open-source tools to meet the needs of your organization
- Manipulate log file formats to make them compatible with various log collectors
- Write new tools to analyze log files and network packets to identify attackers in your environment
- Develop tools that extract otherwise inaccessible forensics artifacts from computer systems of all types
- Automate the collection of intelligence information to augment your security from online resources
- Automate the extraction of signs of compromise and other forensics data from the Windows Registry and other databases
- Write a backdoor that uses exception handling, sockets, process execution, and encryption to provide you with your initial foothold in a target environment. The backdoor will include features such as a port scanner to find an open outbound port, techniques for evading antivirus software and network monitoring, and the ability to embed a payload from tools such as Metasploit.

> **"SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs."**
>
> — Caleb Jaren, **Microsoft**

All security professionals, including penetration testers, forensic analysts, network defenders, security administrators, and incident responders, have one experience in common: CHANGE. Tools, technologies, and threats change constantly, but Python is a simple, user-friendly language that can help you keep pace with change, allowing you to write custom tools and automate tasks to effectively manage and respond to your unique threats.

Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience with or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the course.

Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require. Maybe your chosen Operating System has a new feature that creates interesting forensic artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensic artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold...or you can write a tool yourself.

Or perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization. The answer is simple if you have the skills: Write tools to automate various aspects of your defenses.

As a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool or modify existing capabilities to make them perform as you need them to.

SEC573 is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you to better automate the daily routine of today's information security professional and to achieve more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Learn Python in-depth with us to become fully weaponized.

SEC573: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Essentials Workshop with pyWars

The course begins with a brief introduction to Python and the pyWars Capture-the-Flag game. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. As more advanced students take on Python-based Capture-the-Flag challenges, students who are new to programming will start from the very beginning with Python essentials.

Topics: Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

SECTION 2: Essentials Workshop with MORE pyWars

You will never learn to program by staring at PowerPoint slides. The second section continues the hands-on, lab-centric approach established in Section 1. This section covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and on how to debug your code.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips, Tricks, and Shortcuts; System Arguments; ArgParser Module

SECTION 3: Defensive Python

In this course section, we take on the role of a network defender with more logs to examine than there is time in the day. Attackers have penetrated the network and you will have to analyze the logs and packet captures to find them. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data. Forensicators and offensive security professionals won't be left out because reading and writing files and parsing data are also essential skills they will apply to their craft.

Topics: File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis Tools and Techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

SECTION 4: Hardening Network Services with PowerShell

In this course section, we will use PowerShell and Group Policy to automate the hardening of many exploitable services and protocols, such as Kerberos, Domain Name System (DNS), Remote Desktop Protocol (RDP), and File and Printer Sharing (SMB). Think of Kerberos Golden Tickets, DNS response spoofing, the Bluekeep RDP attack, the EternalBlue/WannaCry SMB worm, and other attacks

Topics: Server Hardening Automation for DevOps; Windows Firewall Scripting; Share Permissions for TCP/UDP Listening Ports with IPsec; Exploitable Protocols and Services

SECTION 4: Forensics Python

In our forensics-themed section, we will assume the role of a forensic analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don't do forensics, you will find that the skills covered in this section are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract those data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then, we will discuss techniques for finding artifacts in other locations, such as SQL databases, and interacting with web pages.

Topics: Acquiring Images from Disk, Memory, and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PIL; SQL Queries; HTTP Communications with Python Built-In Libraries; Web Communications with the Requests Module

SECTION 6: Capture-the-Flag Challenge

In this final section you will be placed on a team with other students to apply the skills you have mastered in a series of programming challenges. Participants will exercise the new skills and the code they have developed throughout the course in a series of challenges. You will solve programming challenges, exploit vulnerable systems, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

Note that students will enjoy this exercise on an individual basis and SANS subject-matter experts are always available to support every student's experience.

Who Should Attend

- Security professionals who benefit from automating routine tasks so they can focus on what's most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

Live Online sans.org/live-online

EVENT	START DATE
Pen Test & Offensive Training	Feb 8
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! SEC460: Enterprise and Cloud | Threat and Vulnerability Assessment

GEVA
Enterprise Vulnerability Assessor
giac.org/geva

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform end-to-end vulnerability assessments
- Develop customized vulnerability discovery, management, and remediation plans
- Conduct threat intelligence gathering and analysis to create a tailored cybersecurity plan that integrates various attack and vulnerability modeling frameworks
- Implement a proven testing methodology using industry-leading tactics and techniques
- Adapt information security approaches to target real-world enterprise challenges
- Configure and manage vulnerability assessment tools to limit risk added to the environment by the tester
- Operate enumeration tools like Nmap, Masscan, Recon-ng, and WMI to identify network nodes, services, configurations, and vulnerabilities that an attacker could use as an opportunity for exploitation
- Conduct infrastructure vulnerability enumeration at scale across numerous network segments, in spite of divergent network infrastructure and nonstandard configurations
- Conduct web application vulnerability enumeration in enterprise environments while solving complex challenges resulting from scale
- Perform manual discovery and validation of cybersecurity vulnerabilities that can be extended to custom and unique applications and systems
- Manage large vulnerability datasets and perform risk calculation and scoring against organization-specific risks
- Implement vulnerability triage and prioritize mitigation
- Use high-end commercial software including Acunetix WVS and Rapid7 Nexpose (InsightVM) in the classroom range

Who Should Attend

- Vulnerability assessors
- IT system administrators
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers

Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from mid-sized to large organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools and a proven testing methodology.

SEC460 takes you beyond the checklist, giving you a tour of the attackers' perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five sections of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test in the final section against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your organization.

> **"SEC460 has provided me the knowledge to build a great vulnerability management/vulnerability assessment program that vendor courses couldn't provide."**
>
> — Eric Osmus, **ConocoPhillips Company**

SEC460: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Vulnerability Management and Assessment

In this section of the course, students will develop the skills needed to conduct high-value vulnerability assessments with measurable impact. We will explore the elemental components of successful vulnerability assessment programs, deconstruct the logistical precursors to value-added operations, and integrate adversarial threat modeling and intelligence.

Topics: Maximizing Value from Vulnerability Assessments and Programs; Setting Up for Success at Scale: Enterprise Architecture and Strategy; Developing Transformational Vulnerability Assessment Strategies; Performing Enterprise Threat Modelling; PowerShell Fundamentals; Generating Compounding Interest from Threat Intelligence and Avoiding Information Overload; The Vulnerability Assessment Framework; Vulnerability Data Management Tools and Techniques; Overview of Comprehensive Network Scanning; Compliance Standards and Information Security; Team Operations and Collaboration; Discovering Open-Source Disclosure and Understanding these Risks

SECTION 3: Enterprise and Cloud Vulnerability Scanning

The third section begins by delving into the next phase of the Vulnerability Assessment Framework and charging into the most exciting topic in security testing: automation to handle scale. We start by breaking vulnerability scanning into its elemental components to gain an understanding of vulnerability measurement that can be applied to task automation. This focus will direct us to the quantitative facets underlying cybersecurity vulnerabilities and drive our discussion of impact, risk, and triage. Each topic discussed will focus on identifying, observing, inciting, or assessing the entry points that threats leverage during network attacks.

Topics: Assigning a Confidence Value and Validating Exploitative Potential of Vulnerabilities; Enhanced Vulnerability Scanning; Risk Assessment Matrices and Rating Systems; Quantitative Analysis Techniques Applied to Vulnerability Scoring; Performing Tailored Risk Calculation to Drive Triage; General Purpose vs. Application-Specific Vulnerability Scanning; Tuning the Scanner to the Task, the Enterprise, and Tremendous Scale; Scan Policies and Compliance Auditing; Performing Vulnerability Discovery with Open-Source and Commercial Appliances; Scanning with the Nmap Scripting Engine, Nexpose/InsightVM, and Acunetix; The Windows Domain: Exchange, SharePoint, and Active Directory; Testing for Insecure Cryptographic Implementations Including SSL; Assessing VOIP Environments; Discovering Vulnerabilities in the Enterprise Backbone: Active Directory, Exchange, and SharePoint; Minimizing Supplemental Risk while Conducting Authenticated Scanning through Purposeful Application of Least Privilege; Probing for Data Link Liability to Identify Hazards in Wireless Infrastructure, Switches, and VLANs; Manual Vulnerability Discovery Automated to Attain Maximal Efficacy; Enterprise Cloud Vulnerability Discovery

SECTION 2: Network and Cloud Asset Discovery and Classification

As the structural foundations of vulnerability management are covered in the first course section, Section 2 will pivot to the realm of direct tactical application. Comprehensive reconnaissance, enumeration, and discovery techniques are the prime elements of successful vulnerability assessment. While gaining additional familiarity with hands-on enterprise operations, you will systematically probe the environment in order to discover the relevant host, service, version, and configuration details that will drive the remainder of the assessment system.

Topics: PowerShell Operations for Discovery; Automating Vulnerability Assessment Tasks with PowerShell; Active and Passive Reconnaissance; Reconnaissance Frameworks; Identification and Enumeration with DNS; DNS Zone Speculation and Dictionary-Enabled Discovery; Port Scanning with Nmap and Zenmap; Scanning Large-Scale Environments; Commonplace Services; Scanning the Network Perimeter and Engaging the DMZ; Trade-offs: Speed, Efficiency, Accuracy, and Thoroughness; The Fundamentals of the Enterprise Cloud; Scanning the Enterprise Cloud

SECTION 4: Vulnerability Validation, Triage, and Mass Data Management

Throughout the fourth section of SEC460, we will tackle vulnerability validation, which is the next phase of our overarching testing methodology. Simultaneously, we will confront and address the biggest headaches common to a vulnerability assessment at scale. At large scale, vulnerability data can be overwhelming and possibly even contradictory. We will cover the specific techniques needed to wade through and better focus those data. Next, we will examine techniques for collaboration and data management with the Acheron tool to analyze vulnerability data across an organization. Later in the section, we will apply our understanding of the vulnerability concept to evolve our PowerShell skills and take action on an enterprise scale.

Topics: Recruiting Disparate Data Sources: Patches, Hotfixes, and Configurations; Manual Vulnerability Validation Targeting Enterprise Infrastructure; Converting Disparate Datasets into a Central, Normalized, and Relational Knowledge Base; Managing Large Repositories of Vulnerability Data; Querying the Vulnerability Knowledge Base; Evaluating Vulnerability Risk in Custom and Unique Systems, including Web Applications; Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk

SECTION 5: Remediation and Reporting

Many well-intentioned Vulnerability Assessment Programs begin with zeal and vitality, but after the discovery of vulnerabilities there is often a tendency to ignore the risk reality and shift back to the status quo. Over the previous course modules we focused on knowing the target environment and uncovering its weak points. Now it's time for decision and action based on an understanding of the risks the organization faces. Developing an actionable vulnerability remediation plan with time-based success targets sets the stage for continuous improvement, and that's exactly what we cover in this section of the course. Developing this plan in conjunction with the Vulnerability Assessment Report is an opportunity to galvanize the team, while enhancing the vulnerability assessment value proposition.

Topics: Analyzing User Password Selection and Addressing Underlying Vulnerabilities; Creating and Navigating Vulnerability Prioritization; Domain Password Auditing; Discovering Negative Security Policy Implementation; Developing a Web of Network and Host Affiliations; Modeling Account Relationships on Active Directory Forests; Designing Vulnerability Mitigations and Compensating Controls; Azure AD Password Protection; Creating Effective Vulnerability Assessment Reports; Transforming Triage Listing into the Vulnerability Remediation Plan; Kerberos and Domain Authentication; Closure: Being a Positive Influence in the Context of the Global Information Security Crisis

SECTION 6: Vulnerability Assessment Hands-on Challenge

In celebration of your diligence, curiosity, and new vulnerability skills, we welcome you to your final hands-on challenge to hammer home your capabilities. The guided scenario in this final section is designed to test your mettle through trial and detailed work in a fun capture-the-flag-style environment. The challenge is the canvas upon which you can hone your skills and measure your maturing talents. Armed for the fight, you will doubtless rise to the challenge...and triumph! The scenario: The Ellingson Mineral Company (EMC) has engaged you to perform a vulnerability assessment of its environment. The organization is very aware of your particular set of vulnerability assessment skills, and treasures the insights it is certain you will provide to help secure the organization against its formidable adversaries, including nefarious cybercrime cartels and jealous nation-state actors. Teams will work together to help squash issues that would lead to a compromise of EMC's precious assets.

Topics: Tactical Employment of the Vulnerability Assessment Framework; Threat Modeling; Discovery; Vulnerability Scanning; Validation; Data Management and Triage

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
Pen Test & Offensive Training	Feb 8
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**

GCIH
Incident Handler
giac.org/gcih

6 Day Program	38 CPEs	Laptop Required

You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

This course enables you to turn the tables on computer attackers by helping you understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. This course will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

You will learn:

- How to best prepare for an eventual breach
- The step-by-step approach used by many computer attackers
- Proactive and reactive defenses for each stage of a computer attack
- How to identify active attacks and compromises
- The latest computer attack vectors and how you can stop them
- How to properly contain attacks
- How to ensure that attackers do not return
- How to recover from computer attacks and restore systems for business
- How to understand and use hacking tools and techniques
- Strategies and tools to detect each type of attack
- Application-level vulnerabilities, attacks, and defenses
- How to develop an incident handling process and prepare a team for battle
- Legal issues in incident handling

> **"I will almost always recommend SEC504 as a baseline so that everyone is speaking the same language. I want my sys-admins to take it, my network admins to take it, even my devs to take it, regardless of whether they're going to eventually move into an incident handling role. In my opinion it is the most critical, foundational class that SANS offers."**
>
> — Kevin Wilcox, **Information Security Specialist**

SEC504: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Incident Response and Computer Crime Investigations

The course starts by examining the key components of both incident response and digital investigations. Informed by several incidents, we consider the goals and outcomes that are important to both business operations and security. The dynamic approach put forth can be applied to the specific needs of an individual business and incident. We then shift to more practical matters, examining issues surrounding live systems and identifying abnormal activity. Continuing the practical focus, we look at investigative techniques for examining evidence from the network and memory. We also cover techniques to determine if an unknown program is malicious, and if so, what footprints are left behind.

Topics: Incident Response; Digital Investigations; Live Examination; Digital Evidence; Network Investigations; Memory Investigations; Malware Investigations

SECTION 3: Password and Access Attacks

This course section starts with straightforward password guessing attacks, quickly investigating the techniques attackers employ to make this an effective process that bypasses defense systems such as account lockout. We will investigate the critical topics of creating effective password guessing lists from other network compromises, and how attackers leverage user password reuse against your organization. We'll dig into the algorithms behind password hashing, using several tools to recover plaintext passwords while optimizing the cracking process to complete in days, not years. We will also get a jump-start on understanding essential network attack topics through the use of easy backdoors, forward and reverse shells, and discrete data transfer within the organization, all through an unassuming system binary. We will also investigate defensive measures that you can immediately apply when you get back to work, including the use of the Domain Password Audit Tool (DPAT) and Elastic Stack (formerly ELK) tools for monitoring authentication logs in your organization.

Topics: Password Attacks; Defense Spotlight: Log Analysis with Elastic Stack (formerly ELK); Understanding Password Hashes; Password Cracking Attacks; Defense Spotlight: Domain Password Auditing; Netcat: The Attacker's Best Friend

SECTION 5: Evasion and Post-Exploitation Attacks

This course section examines the attacker steps after the initial compromise is over. We will dig into the techniques attackers use to implant malware after bypassing endpoint detection and response platforms, how they pivot through the network using third-party and built-in tools, and how they leverage the initial foothold on your network for internal network scanning and asset discovery. We will look at how the compromise of a single host grants attackers privileged network insider access to open up a whole new field of attacks, and how they will use that access wisely, covering their tracks on hosts and on the network to evade detection systems. We will look at how attackers, with their initial access established, then access, collect, and exfiltrate data from compromised networks. We will finish the lecture component of the course with a look at where to go from here in your studies, examining resources and best practices to turn your new skills into permanent, long-term recall.

Topics: Endpoint Security Bypass; Pivoting and Lateral Movement; Privileged Insider Network Attacks; Covering Tracks; Defense Spotlight: Real Intelligence Threat Analytics (RITA); Post-Exploitation Data Collection; Where To Go From Here

SECTION 2: Recon, Scanning, and Enumeration Attacks

This course section covers the details associated with the beginning phases of many cyber attacks. We will introduce important frameworks for understanding the tools, techniques, and practices of modern attackers through the MITRE ATT&CK Framework, using it as a starting point to investigate the pre-attack steps attackers employ. We will leverage local and cloud-based tools to conduct effective reconnaissance of a target organization, identifying the information disclosure that will reveal weaknesses for initial compromise. We'll then take a deep dive into scanning techniques, both from a network perspective and with a focus on the complexities of modern Windows Active Directory forests to map out an attack plan that will grant an attacker privileged access. We will also spotlight defensive techniques using free and open-source tools that provide you with a competitive advantage to detect attacks on your organization.

Topics: Introducing the MITRE ATT&CK Framework; Reconnaissance; Scanning; Enumerating Windows Active Directory Targets; Defense Spotlight: DeepBlueCLI

SECTION 4: Public-Facing and Drive-By Attacks

This course section examines the hacker tools for compromising your exposed systems through exploit frameworks such as Metasploit. We also dig into the concepts and techniques behind drive-by and watering-hole attacks, and how attackers create the exploits and system-compromise tools through malicious installers, browser JavaScript, and malicious Microsoft Office documents. We'll examine the attacks specific to web applications in an organization, both from the perspective of the unauthenticated and the authenticated user, with practical exploit steps for the most popular web application vulnerabilities. In addition to examining the hacker tools, we'll also investigate several freely available and practical defense steps, including the use of the Windows SRUM database for historical system activity reporting, and the use of Elastic Stack (formerly ELK) tools for assessing web server logging data to identify signs of attack.

Topics: Using Metasploit for System Compromise; Drive-By and Watering Hole Attacks; Defense Spotlight: System Resource Usage Monitor (SRUM); Web Application Attacks; Defense Spotlight: Effective Web Server Log Analysis

SECTION 6: Capture-the-Flag Event

Our Capture-the-Flag event is an entire course section filled with hands-on activity that involves you working as a consultant for a fictitious company that has recently been compromised. You will apply all of the skills you've learned in class, using the same techniques attackers use to compromise modern, sophisticated network environments. Working together as teams, small groups will scan, exploit, and complete post-exploitation tasks against a cyber range of target systems including Windows, Linux, Internet of Things, and cloud targets. This hands-on challenge is designed to help players practice their skills and reinforce concepts learned throughout the course while challenging each individual player in an environment that replicates modern networks. Powered by the NetWars engine, the event guides players to successfully compromise target systems, bypass endpoint protection platforms, pivot to internal network high-value hosts, and exfiltrate data that are of greatest value to the target organization. The winners will win the coveted SEC504 challenge coin.

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

> **"SEC504 has been the single best course I have ever taken. It leaves the student prepared and able to understand a broad scope of content in security."**
>
> — Joshua Nielson, **Microsoft**

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
CTI Summit	Jan 25
Cyber Security West: Feb	Feb 1
Pen Test & Offensive Training	Feb 8
Cyber Security East: Feb	Feb 22
Cyber Security East: March	Mar 1
Cyber Security West: March	Mar 15
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
Pen Test Austin: Virtual Edition	Apr 19
Baltimore Spring: Virtual Edition	Apr 26
Cyber Security Central: May	May 3
Security West	May 10
Purple Team Summit	May 17
Cyber Security Central: June	Jun 7
SOC Training	Jun 14
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC542: **Web App Penetration Testing and Ethical Hacking**

GWAPT
Web Application Penetration Tester
giac.org/gwapt

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Apply OWASP's methodology to your web application penetration tests to ensure they are consistent, reproducible, rigorous, and under quality control
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization
- Understand and exploit insecure deserialization vulnerabilities with ysoserial and similar tools
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and BurpSuite Pro to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform two complete web penetration tests, one during the five course instruction sections, and the other during the Capture the Flag exercise

Who Should Attend

- General security Practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers, architects, and developers

Web applications play a vital role in every modern organization. But if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the business impact should attackers exploit the discovered vulnerabilities.

Students will come to understand common web application flaws, as well as how to identify and exploit them with the intent of demonstrating the potential business impact. Along the way, students follow a field-tested and repeatable process to consistently find flaws. Information security professionals often struggle with helping organizations understand risk in terms relatable to business. Executing awesome hacks is of little value if an organization does not take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help students demonstrate the true impact of web application flaws not only through exploitation but also through proper documenting and reporting.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to walking students through a web app penetration through the use of more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture the Flag event on the final section brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way to hammer home lessons learned.

> **"SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool, or that tool."**
>
> — Christopher J. Stover, **Infogressive Inc.**

SEC542: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Introduction and Information Gathering

Understanding the attacker's perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients, and server architectures, from the attacker's perspective. We look at collecting open-source intelligence (OSINT) specific to data points likely to help exploitation be more successful. We analyze the importance of encryption and HTTPS. Before leaving HTTPS, we dive into the infamous Heartbleed flaw and get our first taste of exploitation with a hands-on lab. We look at the methodology promoted by OWASP to help ensure the delivery of high-quality assessments, as well as the things necessary for a penetration tester's toolkit. The most important tool, an interception proxy, is introduced through performing the initial configuration steps in OWASP's Zed Attack Proxy (ZAP) and BurpSuite Professional. To complete the section, we explore aspects of a vulnerable web application using BurpSuite.

Topics: Overview of the Web from a Penetration Tester's Perspective; Web Application Assessment Methodologies; The Penetration Tester's Toolkit; WHOIS and DNS Reconnaissance; Open-Source Intelligence (OSINT); The HTTP Protocol; Secure Sockets Layer (SSL) Configurations and Weaknesses; Interception Proxies; Proxying SSL Through BurpSuite Pro and Zed Attack Proxy; Heartbleed Exploitation

SECTION 3: Injection

After ending Section 2 with a successful authentication event, we begin by exploring how web applications track authenticated users and ways to exploit weaknesses in session management. We discuss authentication and authorization bypasses, which can expose sensitive data and business functions to attackers, as well as exploit an authentication flaw in Mutillidae. We will build on the information identified during the target profiling, spidering, and forced browsing exercises, exploring methods to find and verify vulnerabilities within the application. Students also begin to explore the interactions between the various vulnerabilities. This course section dives deeply into vital manual testing techniques for vulnerability discovery. We focus on developing in-depth knowledge of interception proxies for web application vulnerability discovery. Many of the most common injection flaws (command injection and local and remote file inclusion) are introduced, and followed with lab exercises, to reinforce the discovery and exploitation. Besides this, a section covers insecure deserialization, a common vulnerability in object-oriented programming languages, where students will exploit a Java insecure deserialization vulnerability in a lab in order to steal a secret file from a vulnerable web application. Due to its prevalence and the significant impact generally associated with the flaw, a large portion of the section is devoted to traditional and blind SQL injection.

Topics: Session Management and Attacks; Authentication and Authorization Bypass; Mutillidae; Command Injection; Directory Traversal; Local File Inclusion (LFI); Remote File Inclusion (RFI); Insecure Deserialization; SQL Injection; Blind SQL Injection; Error-based SQL Injection; Exploiting SQL Injection; SQL Injection Tools: sqlmap

SECTION 2: Configuration, Identity, and Authorization Testing

Section 2 begins with profiling the target(s) to understand the underlying configuration. The collected data is used to build a profile of each server and identify potential configuration flaws. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance and use the Shellshock vulnerability to exploit a configuration flaw against in-class targets. The exploitation is an opportunity to get deeper hands-on experience with BurpSuite Pro, cURL, and manual exploitation techniques. The system's configuration should involve proper logging and monitoring to ensure security-related events are not missed. We will briefly explore logging configuration and basic incident response testing. We build a map or diagram of the application's pages and features. This phase involves identifying the components, analyzing the relationship between them, and determining how the pieces work together. We then dive deep into the spidering/crawling results, which represents a vital part of the overall penetration test, as well as perform forced browsing in a lab to find hidden content. Towards the end of the section, we examine different authentication systems, including Basic, Digest, Forms, Windows Integrated and OAuth authentication, and discuss how servers use them and attackers abuse them. We will perform username enumeration and in the final exercise, we will use Burp's fuzzer, Intruder, to guess the password used to successfully authenticate to a web application.

Topics: Target Profiling; Collecting Server Information; Logging and Monitoring; Learning Tools to Spider a Website; Analyzing Website Contents; Brute Forcing Unlinked Files and Directories; Fuzzing; Web Authentication Mechanisms; Username Harvesting and Password Guessing; Burp Intruder

SECTION 4: XXE and XSS

In Section 4, students continue exploring injection flaws. We cover methods to discover key vulnerabilities within web applications, such as XML External Entities (XXE). After XXE, the rest of the section is devoted to introducing Cross-Site Scripting (XSS) vulnerabilities, including reflected, stored and DOM-based XSS vulnerabilities. Manual discovery methods are employed during hands-on labs. Section 4 also introduces BeEF to students, which is used in a lab. The course continues with a detailed discussion of AJAX as we explore how it enlarges the attack surface leveraged by penetration testers. We also analyze how AJAX is affected by other vulnerabilities already covered in depth earlier in the course. Finally, the section ends with a lab in which an AJAX web application is exploited, and finally hooked with BeEF for total control.

Topics: XML External Entity (XXE); Cross-Site Scripting (XSS); Browser Exploitation Framework (BeEF); AJAX; XML and JSON; Document Object Model (DOM); Logic Attacks; API Attacks; Data Attacks

SECTION 5: CSRF, Logic Flaws, and Advanced Tools

In Section 5, we launch actual exploits against real-world applications, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of web application penetration testing. During our exploitation phase, we expand our use of tools such as ZAP and BurpSuite Pro, plus complement them with further use of sqlmap and Metasploit to help craft exploits against various web applications. We launch SQL injection and Cross-Site Request Forgery attacks, among others. In class we exploit these flaws to perform data theft, hijack sessions, deface a website, get shells, pivot against connected networks, and much more. Through various forms of exploitation, the student gains a keen understanding of the potential business impact of these flaws to an organization. While the whole course is geared towards understanding how web application vulnerabilities work and how they can be exploited, in Section 5 we also introduce the active scanner component in BurpSuite Pro. We wrap up section instruction by reviewing how to prepare for penetration testing assessments and important post-assessment activities, such as report writing.

Topics: Cross-Site Request Forgery (CSRF); Python for Web App Penetration Testing; WPScan; ExploitDB; BurpSuite Pro Scanner; Metasploit; When Tools Fail; Business of Penetration Testing

SECTION 6: Capture the Flag

In Section 6, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag exercise provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated-hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Pen Test & Offensive Training	Feb 8
Cyber Security East: March	Mar 1
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
Cyber Security East: May	May 17
Cyber Security Central: June	Jun 7
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC560: **Network Penetration Testing and Ethical Hacking**

GPEN
Penetration Tester
giac.org/gpen

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources
- Utilize the Nmap scanning tool to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Analyze the output of scanning tools and perform false positive reduction using Netcat and the Scapy packet crafting tools
- Utilize the Windows and Linux command lines to plunder target systems
- Configure the Metasploit exploitation tool to scan, exploit, and then pivot through a target environment in-depth
- Perform Kerberos attacks including Kerberoasting, Golden Ticket, and Silver Ticket attacks
- Use Mimikatz to perform domain domination attacks, such as golden ticket abuse, DCSync, and others
- Attack Azure AD and use your domain domination to target the on-premise integration

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red Team members
- Blue Team members
- Forensics specialists who want to better understand offensive tactics
- Incident responders who want to understand the mind of an attacker

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 IS THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step by step and end to end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, Windows Domain attacks, and Azure AD (Active Directory), with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently, and with great skill.

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

You'll learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and the Windows domain, pivoting through the target environment to model the attacks of real-world adversaries to emphasize the importance of defense in depth.

EQUIPPING SECURITY ORGANIZATIONS WITH COMPREHENSIVE PENETRATION TESTING AND ETHICAL HACKING KNOW-HOW

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test and at the end of the course you'll do just that. After building your skills in comprehensive and challenging labs, the course culminates with a final real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the skills you've gained in this course.

> **"SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective."**
>
> — Steve Nolan, **General Dynamics**

SEC560: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Comprehensive Pen Test Planning, Scoping, and Recon

In this course section, you'll develop the skills needed to conduct a best-of-breed, high-value penetration test. We'll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We'll then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We'll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on lab exercises to learn about a target environment, as well as a lab using Spiderfoot to automate the discovery of information about the target organization, network, infrastructure, and users.

Topics: The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Mining Search Engine Results; Reconnaissance of the Target Organization, Infrastructure, and Users; Automating Reconnaissance with Spiderfoot

SECTION 3: Exploitation

In this course section we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We'll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You'll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments. You'll also analyze the topic of anti-virus evasion to bypass the target organization's security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

Topics: Comprehensive Metasploit Coverage with Exploits, Stagers, and Stages; Strategies and Tactics for Anti-Virus Evasion and Application Control Bypass; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage PowerShell Empire to Plunder a Target Environment; Lateral Movement with WMI and SC

SECTION 2: In-Depth Scanning

This course section focuses on the vital task of mapping the target environment's attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We finish the module covering vital techniques for false-positive reduction, so you can focus your findings on meaningful results and avoid the sting of a false positive. And we examine the best ways to conduct your scans safely and efficiently.

Topics: Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth: The Nmap Scripting Engine; Version Scanning with Nmap; Identifying Insecurities in Windows with GhostPack Seatbelt; False-Positive Reduction; Netcat for the Pen Tester; Initial Access; Password Guessing, Spraying, and Credential Stuffing

SECTION 4: Password Attacks and Merciless Pivoting

Once you've successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. This course section zooms in on pillaging target environments and building formidable hands-on command line skills. We'll then turn our attention to password cracking attacks, as well as numerous options for plundering password hashes from target machines, including the great Mimikatz Kiwi tool. We'll cover password cracking techniques and strategies using both John the Ripper and Hashcat. In addition, we'll look at pivoting techniques using SSH and the routing features in Metasploit. We'll cover Windows command line skills in-depth, including PowerShell's awesome abilities for post-exploitation. The course section wraps up with a discussion on effective reporting and communication with the business.

Topics: Password Attack Tips; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi; PowerShell's Amazing Post-Exploitation Capabilities; Tips for Effective Reporting

SECTION 5: Domain Domination and Web App Pen Testing

In this course section, we'll zoom in on typical Active Directory lateral movement strategies. You'll get an in-depth understanding of how Kerberos works and what the possible attack vectors are. We'll look at typical local privilege escalation techniques and User Account Control bypasses. We'll also map the internal domain structure using BloodHound to identify feasible attack paths. We'll use Mimikatz to perform domain dominance attacks, where domain replication is used to fully compromise the domain. With full privileges over the on-premise domain, we'll then turn our attention to the cloud and have a look at Azure principles and attack strategies. The integration of Azure AD with the on-premise domain provides interesting attack options, which will be linked to the domain dominance attacks we saw earlier during the course section.

Topics: Kerberos Authentication Protocol; Poisoning Multicast Name Resolution with Responder; Domain Mapping and Exploitation with Bloodhound; Effective Domain Privilege Escalation; Persistent Administrative Domain Access; Azure Authentication Principles and Attacks; Azure AD Integration with On-Premise Domain; Azure Applications and Attack Strategies

SECTION 6: Penetration Test and Capture-the-Flag Workshop

This lively session represents the culmination of the network penetration testing and ethical hacking course. You'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop during which you'll conduct an actual penetration test of a sample target environment. We'll provide the scope and rules of engagement, and you'll work with a team to achieve your goal of finding out whether the target organization's Personally Identifiable Information (PII) is at risk. As a final step in preparing you for conducting penetration tests, you'll make recommendations about remediating the risks you identify.

Topics: Applying Penetration Testing and Ethical Hacking Practices End-to-End; Detailed Scanning to Find Vulnerabilities and Avenues to Entry; Exploitation to Gain Control of Target Systems; Post-Exploitation to Determine Business Risks; Merciless Pivoting; Analyzing Results to Understand Business Risk and Devise Corrective Actions

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Pen Test & Offensive Training	Feb 8
Cyber Security East: March	Mar 1
Cyber Security West: March	Mar 15
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
Cyber Security East: April	Apr 12
Pen Test Austin: Virtual Edition	Apr 19
Rocky Mountain Spring	Apr 26
Security West	May 10
Purple Team Summit	May 17
Cyber Security Central: June	Jun 7
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC575: **Mobile Device Security and Ethical Hacking**

GMOB
Mobile Device Security Analyst
giac.org/gmob

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android file system data to plunder compromised devices and extract sensitive mobile device use information
- Analyze Apple iOS and Android applications with reverse-engineering tools
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- Conduct an automated security assessment of mobile applications
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

> **"SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers."**
>
> — Richard Takacs, **Integrity360**

Imagine an attack surface that is spread across your organization and in the hands of every user. It moves regularly from place to place, stores highly sensitive and critical data, and sports numerous and different wireless technologies all ripe for attack. Unfortunately, such a surface already exists today: mobile devices. These devices constitute the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills to understand the security strengths and weaknesses of Apple iOS and Android devices. Mobile devices are no longer a convenience technology – they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores across the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too. The SEC575 course examines the full gamut of these devices.

With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and manipulate apps to circumvent client-side security techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS, and you'll bypass lock screen to exploit lost or stolen devices.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review ways to effectively communicate threats to key stakeholders. You'll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks for in-house applications.

In employing your newly learned skills, you'll apply a step-by-step mobile device deployment penetration test. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step of the test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as someone prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

SEC575: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Device Architecture and Application Interaction

The first section of SEC575 looks at the significant threats affecting mobile device deployments, highlighted by a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities between Android (including Android 10) and Apple iOS 13. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data. Finally, we will examine how applications interact with each other, as application interaction creates an interesting attack surface for mobile penetration tests.

Topics: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Mobile Application Interaction; Mobile Device Lab Analysis Tools

SECTION 3: Static Application Analysis

One of the core skills you need as a mobile security analyst is the ability to evaluate the risks and threats a mobile app introduces to your organization. The lectures and hands-on exercises presented in this course section will enable you to use your analysis skills to evaluate critical mobile applications to determine the type of access threats and information disclosure threats they represent. We will use automated and manual application assessment tools to statically evaluate iOS and Android apps. Initially, the applications will be easy to understand, but towards the end of the section we will dig into obfuscated applications that are far more difficult to dissect. Finally, we will examine different kinds of application frameworks and how they can be analyzed with specialized tools.

Topics: Reverse-Engineering Obfuscated Applications; Static Application Analysis; Third-Party Application Frameworks

SECTION 5: Mobile Penetration Testing

After having analyzed the applications both statically and dynamically, one component is still left untouched: the back-end server. In this course section we will examine how you can perform ARP spoofing attacks on a network in order to obtain a man-in-the-middle position, and how Android and iOS try to protect users from having their sensitive information intercepted. Next, we'll examine how you can set up a test device to purposely intercept the traffic in order to find vulnerabilities on the back-end server. We end the section by creating a RAT application that can be used during a red team assessment in order to target users and gain access to internal networks.

Topics: Network Manipulation Attacks; SSL/TLS Attacks; Web Framework Attacks; Using Mobile Device Remote Access Trojans

SECTION 2: The Stolen Device Threat and Mobile Malware

A very important threat for mobile devices is the stolen or lost device, as this can cause a major disclosure of sensitive information. In this course section we first examine how a device can be properly protected, and how someone might be able to circumvent those protections. Once access to the device has been obtained, we examine which information is available and how we can access it. On the other hand, gaining privileged access to a device is often needed to perform a security assessment, so we will take a look at the steps required to root an Android phone and jailbreak an iOS device. At the end of the section, we will take a look at how mobile malware (ab)uses the ecosystem to steal money or data or brick the device.

Topics: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and File System Architecture; Mobile Device Malware Threats

SECTION 4: Dynamic Mobile Application Analysis and Manipulation

After having performed static analysis on applications in Section 3, we now move on to dynamic analysis. A skilled analyst combines both static and dynamic analysis to evaluate the security posture of an application. Using dynamic instrumentation frameworks, we see how applications can be modified at runtime, how method calls can be intercepted and modified, and how we can have direct access to the native memory of the device. We will learn about Frida, Objection, Needle, Drozer, and method swizzling to fully instrument and examine both Android and iOS applications. The section ends with a look at a consistent system for evaluating and grading the security of mobile applications using the Application Report Card Project. By identifying these flaws we can evaluate the mobile phone deployment risk to the organization with practical and useful risk metrics. Whether your role is to implement the penetration test or to source and evaluate the penetration tests of others, understanding these techniques will help you and your organization identify and resolve vulnerabilities before they become incidents.

Topics: Manipulating and Analyzing iOS Applications; Manipulating and Analyzing Android Applications; Application Report Cards

SECTION 6: Hands-on Capture-the-Flag Event

In the final section of SEC575 we will pull together all the concepts and technology covered throughout the course in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will examine multiple applications and forensic images to identify weaknesses and sources of sensitive information disclosure, and analyze obfuscated malware samples to understand how they work. During this mobile security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

> **"In the fast-paced world of bring-your-own devices and mobile device management, SEC575 is a must-have course for InfoSec managers."**
>
> — Jude Meche, **DSCC**

Live Online sans.org/live-online

EVENT	START DATE
Pen Test & Offensive Training	Feb 8
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Miami: Virtual Edition	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! SEC588: **Cloud Penetration Testing**

GCPN
Cloud Penetration Tester
giac.org/gcpn

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Conduct cloud based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand first-hand how cloud environments are constructed and how to scale factors into the gathering of evidence

Author Statement

"When I was first asked about putting together a cloud penetration testing class, there were many questions. Could there be room for a class as 'niche' as this? We felt the need to have a class with all new material and topics that we had not covered in any of our other penetration testing classes. I believe we have met that need with this class in ways most could not have imagined. This class breaks the rules and allows us to help you test, assess, and secure cloud environments."
— Moses Frost

Computing workloads have been moving to the cloud for years. Analysts predict that most if not all companies will have workloads in public and other cloud environments in the very near future. While organizations that start in a cloud-first environment may eventually move to a hybrid cloud and local data center solution, cloud usage will not decrease significantly. So when it comes to assessing risk to organizations, we need to be prepared to assess the security of cloud-delivered services. In this course you will learn the latest in penetration testing techniques focused on the cloud and how to assess cloud environments.

The most commonly asked questions regarding cloud security are "Do I need training for cloud-specific penetration testing" and "Can I accomplish my objectives with other pen test training and apply it to the cloud?" The answer to both questions is yes, but to understand why, we need to address the explicit importance of having cloud-focused penetration testing. In cloud-service-provider environments, penetration testers will not encounter a traditional data center design. Specifically, what we rely on to be true in a traditional setting – such as who owns the Operating System, who owns the infrastructure, and how the applications are running – will likely be very different. Applications, services, and data will be hosted on a shared hosting environment that is potentially unique to each cloud provider.

What makes cloud native different? The Cloud Native Computing Foundation, which was chartered to provide guidance on defining a cloud-first and cloud-native application, states that the application and environment will be composed of containers, service meshes, microservices, immutable infrastructure, and declarative APIs.

While some of these items are available in a non-cloud environment, in the cloud these features are further decomposed into services that are made available by cloud providers. In this environment, an example of complexity is a microservices architecture in which there may be a virtual machine, a container, or even what is considered a "serverless" hosting area. We must therefore deal with additional complexity in order to appropriately assess this environment, stay within the legal bounds, and learn new and different ways to perform what we would consider legacy attacks.

SEC588 dives into these topics as well as other new topics that appear in the cloud like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. The course also specifically covers Azure and Amazon Web Services (AWS) penetration testing, which is particularly important given that AWS and Microsoft account for more than half of the market. The goal is not to demonstrate these technologies, but rather to teach you how to assess and report on the true risk that the organization could face if these services are left insecure.

> **"SEC588 taught me more than I expected. With the rapid development of new technologies offered by cloud providers, SEC588 has given me an important framework for cloud pen testing."**
>
> — Jonus Gerrits; **Phillips 66**

SEC588: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Discovery, Recon, and Architecture at Scale

In this course section you will be conducting the first phases of a Cloud-Focused Penetration Testing Assessment. We'll get familiar with how the terms of service, demarcation points, and limits imposed by cloud service providers function. There are labs on how open databases and Internet-level scans can be used in near real time as well as historically to uncover target infrastructure and vulnerabilities. In this course section we'll describe how web scale affects reconnaissance and how we can best address it. The exercises are designed to walk through the discovery of useful artifacts and the labs themselves throughout the course – a virtual hacker treasure hunt!

Topics: Cloud Assessment Methodology; Infrastructure Cloud Components; Terms of Service and Demarcation Points; Domains and Certificates for Enumeration; Host Discovery with MassCAN and Nmap; Git Mirroring; Services and Databases in the Cloud; Recon and Discovery through Visual Tracking

SECTION 2: Mapping, Authentication, and Cloud Services

In this course section, we'll show the differences between mapping at the port level, application level, and infrastructure mapping through cloud-service-provider APIs. The section features labs designed to show how we can go from outer to inner reconnaissance and discovery. We'll then shift to three very important and interrelated topics: authentication and authorization in APIs, identifying undisclosed APIs and how they can be used, and how to abuse privilege and identity management. Amazon Web Services and other cloud providers have adopted an RBAC system to which many of their services can turn to for authorization checking. The last part of this section will cover privileges in RBAC and how we can abuse them to elevate privileges. Our labs will show how a low-privilege user can run lambda functions, enumerate s3 buckets, execute ec2 instances, and even decrypt sensitive data.

Topics: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and File System Architecture; Mobile Device Malware Threats

SECTION 3: Azure and Windows Services in the Cloud

While Amazon Web Services holds the largest share of the market, many large enterprises are moving their on-premise workloads into the cloud. Microsoft Azure, while being equivalent to many other cloud providers, also has some unique services that are used. Azure Active Directory and other user services such as Office365, Exchange, and even Microsoft Graph are unique in their services. This section will introduce you to an Azure Environment in which we have provided Windows machines, containers, and services. As during the previous course sections, the environments are live and running, and each has its own set of artifacts to run through. We will leverage similar CLI tooling to take over Azure services in a controlled manner.

Topics: Azure Active Directory; VHD and Volume Shadow Copies; SAML and Microsoft ADFS; Windows Containers; Azure Roles; Microsoft Graph API; Office365

SECTION 4: Vulnerabilities in Cloud Native Applications

The fourth section of this course focuses on what are referred to as cloud native applications. While the instruction particularly examines web applications themselves, it is designed to show how cloud native applications operate and how we can assess them. More and more, what we see being created in the wild are applications that are container-packaged and microservice-oriented. These applications will have their nuances. They will typically be deployed in a service mesh at times that could indicate a system like Kubernetes is used. We will be exploring many questions in this section, including:

- Which application vulnerabilities are very critical in your environments?
- How does Serverless and Lambda change your approach?
- How does managed and unmanaged Kubernetes change your testing?
- How do microservice applications operate?
- What is the CI/CD pipeline and how can it be abused?

Topics: AWS IAM Metadata Discovery; Kubernetes and Escapes; TravisCI and Git Actions; Moving Laterally Across Containers; Privileged and Unprivileged Containers

SECTION 5: Exploitation and Red Team in the Cloud

The final section of this course explores the world of exploitation and red teaming in the cloud. By this time we have a very good understanding of our target environments, and as such we will explore how we can exploit what we have found, advance further into the environments, and finally how to move around laterally. This includes breaking out of containers and service meshes and exfiltrating data in various ways to show the real business impact of these types of attacks.

Topics: Red Team and Methodologies; Heavy and Lite Shells; Data Smuggling; Avoiding Detections

SECTION 6: Capstone

Be prepared during your final course section to work as a team and complete an end-to-end assessment in a new cloud environment. The applications and environments are all newly designed to imitate real-world environments. This section is designed to allow students to put together the week's worth of knowledge, reinforcing theory and practice, and simulating an end-to-end test. It is also a capstone event, as we will be asking students to write a report using a method that is easy to read for both developers and administrative staff. We will provide students with a few rubrics and ways to work through the scenarios. There are always new and novel solutions and we like students to share what they have learned and how they did what they did with each other.

Who Should Attend

- Attack-focused and defense-focused security practitioners will benefit greatly from this course by gaining a deep understanding of vulnerabilities, insecure configurations, and associated business risk to their organizations
- Penetration testers
- Vulnerability analysts
- Risk assessment officers
- DevOps engineers
- Site reliability engineers

> **"This emerging course perfectly complements the change in the direction of red team engagement scopes."**
>
> — Kyle Spaziani, **Sanofi**

Live Online sans.org/live-online

EVENT	START DATE
Cloud Defender	Jan 11
Pen Test & Offensive Training	Feb 8
Cyber Security East: March	Mar 1
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
CloudSec Next Summit	Jun 7
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC599: **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses**

GDAT
Defending Advanced Threats
giac.org/gdat

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Understand how recent high-profile attacks were delivered and how they could have been stopped
- Implement security controls throughout the different phases of the Cyber Kill Chain and the MITRE ATT&CK framework to prevent, detect, and respond to attacks

> **"SEC599 gave me interesting insight into Exploit Guard that will certainly drive great conversation at work. Best labs of any class I've taken."**
>
> — Jeremiah Hainly,
> **The Hershey Company**

You just got hired to help our virtual organization "SYNCTECHLABS" build out a cybersecurity capability. On your first day, your manager tells you: "We looked at some recent cybersecurity trend reports and we feel like we've lost the plot. Advanced persistent threats, ransomware, denial of service...We're not even sure where to start!"

Cyber threats are on the rise: ransomware tactics are affecting small, mid-size, and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses will arm you with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries.

Course authors Stephen Sims and Erik Van Buggenhout (both certified as GIAC Security Experts) are hands-on practitioners who have built a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked the question: "How do I prevent or detect this type of attack?" Well, this is it! SEC599 gives students real-world examples of how to prevent attacks. The course features more than 20 labs plus a full-day Defend-the-Flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment.

Our six-part journey will start off with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, you will also compromise our virtual organization "SYNCTECHLABS" in section one exercises.

In sections two, three, four, and five we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. The topics to be addressed include:

- Leveraging MITRE ATT&CK as a "common language" in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for script controls (Unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

SEC599 will finish with a bang. During the Defend-the-Flag challenge in the final course section, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren't slowing down, so what are you waiting for?

SEC599: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Introduction & Reconnaissance

Our six-part journey starts with an analysis of recent attacks through in-depth case studies. We will explain what's happening in real situations and introduce the Cyber Kill Chain and MITRE ATT&CK framework as a structured approach to describing adversary tactics and techniques. We will also explain what purple teaming is, typical tools associated with it, and how it can be best organized in your organization. In order to understand how attacks work, students will also compromise our virtual organization "SYNCTECHLABS" during Section 1 exercises.

Topics: Course Outline and Lab Setup; Adversary Emulation and the Purple Team; Reconnaissance

SECTION 2: Payload Delivery and Execution

Section 2 will cover how the attacker attempts to deliver and execute payloads in the organization. We will first cover adversary techniques (e.g., creation of malicious executables and scripts), then focus on how both payload delivery (e.g., phishing mails) and execution (e.g., double-clicking of the attachment) can be hindered. We will also introduce YARA as a common payload description language and SIGMA as a vendor-agnostic use-case description language.

Topics: Common Delivery Mechanisms; Hindering Payload Delivery; Preventing Payload Execution

SECTION 3: Exploitation, Persistence, and Command and Control

Section 3 will first explain how exploitation can be prevented or detected. We will show how security should be an integral part of the software development lifecycle and how this can help prevent the creation of vulnerable software. We will also explain how patch management fits in the overall picture. Next, we will zoom in on exploit mitigation techniques, both at compile-time (e.g., ControlFlowGuard) and at run-time (ExploitGuard). We will provide an in-depth explanation of what the different exploit mitigation techniques (attempt to) cover and how effective they are. We'll then turn to a discussion of typical persistence strategies and how they can be detected using Autoruns and OSQuery. Finally, we will illustrate how command and control channels are being set up and what controls are available to the defender for detection and prevention.

Topics: Protecting Applications from Exploitation; Avoiding Installation; Foiling Command and Control

SECTION 4: Lateral Movement

Section 4 will focus on how adversaries move laterally throughout an environment. A key focus will be on Active Directory (AD) structures and protocols (local credential stealing, NTLMv2, Kerberosm, etc.). We will discuss common attack strategies, including Windows privilege escalation, UAC bypasses, (Over-) Pass-the-Hash, Kerberoasting, Silver Tickets, and others. We'll also cover how BloodHound can be used to develop attack paths through the AD environment. Finally, we will discuss how lateral movement can be identified in the environment and how cyber deception can be used to catch intruders red-handed!

Topics: Protecting Administrative Access; Key Attack Strategies against AD; How Can We Detect Lateral Movement?

SECTION 5: Action on Objectives, Threat Hunting, and Incident Response

Section 5 focuses on stopping the adversary during the final stages of the attack:

- How does the adversary obtain "domain dominance" status? This includes the use of Golden Tickets, Skeleton Keys, and directory replication attacks such as DCSync and DCShadow.
- How can data exfiltration be detected and stopped?
- How can threat intelligence aid defenders in the Cyber Kill Chain?
- How can defenders perform effective incident response?

As always, theoretical concepts will be illustrated during the different exercises performed throughout the section.

Topics: Domain Dominance; Data Exfiltration; Leveraging Threat Intelligence; Threat Hunting and Incident Response

SECTION 6: APT Defender Capstone

The course culminates in a team-based Defend-the-Flag competition. Section 6 is a full chapter of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls promoted all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge. Note that students will enjoy this exercise on an individual basis and SANS subject-matter experts are always available to support every student's experience.

Topics: Applying Previously Covered Security Controls In-depth; Reconnaissance; Weaponization; Delivery; Exploitation; Installation; Command and Control; Action on Objectives

Who Should Attend

- Security architects and security engineers who want to better understand how the defenses they put in place make an impact on adversary operations
- Red teamers and penetration testers who want to better understand how blue team techniques could stop their attacks
- Technical security managers who want to understand what security controls should be prioritized
- Security Operations Center analysts and engineers who want to better understand how they can detect adversary techniques
- Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents.

> **"SEC599 gives really good background about adversary behavior and the steps needed to detect it."**
>
> — Tarot Wake,
> **Halkyn Consulting Ltd**

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
CTI Summit	Jan 25
Scottsdale: Virtual Edition	Feb 22
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
Purple Team Summit	May 17
SOC Training	Jun 14

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC617: **Wireless Penetration Testing and Ethical Hacking**

GAWN
Assessing & Auditing Wireless Networks
giac.org/gawn

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless devices to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones
- Implement a WPA2 Enterprise penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilize Scapy to force custom packets to manipulate wireless networks in new ways, quickly building custom attack tools to meet specific penetration test requirements
- Identify WiFi attacks using network packet captures traces and freely available analysis tools
- Identify and exploit shortcomings in the security of proximity key card systems
- Decode proprietary radio signals using Software-Defined Radio
- Mount a penetration test against numerous standards-based or proprietary wireless technologies

Who Should Attend

- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

Course Preview available at: **sans.org/demo**

This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organizations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, assess, and defend against these threats. These are "must-have" skills for any high-performing security organization.

For many analysts, "wireless" was once synonymous with "Wi-Fi," the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of Wi-Fi systems, but also the security of Bluetooth, Zigbee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of Wi-Fi networks and identify the Wi-Fi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern Wi-Fi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in Wi-Fi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking Wi-Fi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android Wi-Fi stacks.

SEC617 is a technical, hands-on penetration testing skill-development course that requires a wide variety of super-useful hardware and software tools to successfully build new skills. In this course, you will receive the SANS Wireless Assessment Toolkit (SWAT), which is a collection of hardware and software tools that will jumpstart your ability to assess wireless systems. The toolkit includes a high-powered 802.11b/g/n Wi-Fi card, a long-range Bluetooth Classic/Low Energy adapter, a high-frequency RFID reader and writer, and a software-defined radio receiver. You will also receive a customized Linux software environment so you can work on assessing systems and avoid fighting hardware/software incompatibility.

> **"I have a better understanding of the technologies and protocols in use and can now perform more accurate risk assessments."**
>
> — Shawn Pray, **Accenture**

Live Online **sans.org/live-online**

EVENT	START DATE
Pen Test & Offensive Training	Feb 8
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Cyber Security East: May	May 17

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! SEC642: **Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Perform advanced Local File Include (LFI)/Remote File Include (RFI), Blind SQL injection (SQLi), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

Who Should Attend

- Web and network penetration testers
- Red team members
- Vulnerability assessment personnel
- Security consultants
- Developers, QA testers
- System administrators and IT managers
- System architects

Course Preview available at: **sans.org/demo**

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever-more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets at a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course section culminates in a Capture-the-Flag competition where you will apply the knowledge you acquired during the previous five sections in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

> **"SEC642 is quality content for senior penetration testers – a nice extension of standard WAPT courses!"**
>
> — Caleb Jaren, **Microsoft**

Live Online sans.org/live-online

EVENT	START DATE
Pen Test & Offensive Training.	Feb 8
Pen Test Austin: Virtual Edition . .	Apr 19

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**

GXPN
Exploit Researcher & Advanced Pen Tester
giac.org/gxpn

6	46	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse-engineer vulnerable code to write custom exploits

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

> **"SEC660 is the right balance between theory and practice; it's hands-on, not too hard, but also not too easy."**
>
> — Anton Ebertzeder, **Siemens AG**

This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each section includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of section one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, SSL, ARP, and others. Section 2 starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the section is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Section 3 jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Sections 4 and 5 are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course section is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

Among the biggest benefits of SEC660 is the expert-level hands-on guidance provided through the labs and the additional time allotted each evening to reinforce daytime material and master the exercises.

SEC660: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Network Attacks for Penetration Testers

Section 1 serves as an advanced network attack module, building on knowledge gained from SEC560. The focus will be on obtaining access to the network; manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

Topics: Bypassing Network Admission Control; Impersonating Devices with Admission Control Policy Exceptions; Exploiting EAP-MD5 Authentication; Custom Network Protocol Manipulation with Ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; Exploiting OSPF Authentication to Inject Malicious Routing Updates; Using Evilgrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip; Remote Cisco Router Configuration File Retrieval; IPv6 for Penetration Testers

SECTION 2: Crypto and Post-Exploitation

Section 2 starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We finish the module with lab exercises that allow you to practice your new-found crypto attack skill set against reproduced real-world application vulnerabilities.

Topics: Pen Testing Cryptographic Implementations; Exploiting CBC Bit Flipping Vulnerabilities; Exploiting Hash Length Extension Vulnerabilities; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Using PXE, Network Attacks, and Local Privilege Escalation

SECTION 3: Python, Scapy, and Fuzzing

Section 3 starts with a focus on how to leverage Python as a penetration tester. It is designed to help people unfamiliar with Python start modifying scripts to add to their own functionality while helping seasoned Python scripters improve their skills. Once we leverage the Python skills in creative lab exercises, we move on to leveraging Scapy for custom network targeting and protocol manipulation. Using Scapy, we examine techniques for transmitting and receiving network traffic beyond what canned tools can accomplish, including IPv6.

Topics: Becoming Familiar with Python Types; Leveraging Python Modules for Real-World Pen Tester Tasks; Manipulating Stateful Protocols with Scapy; Using Scapy to Create a Custom Wireless Data Leakage Tool; Product Security Testing; Using Taof for Quick Protocol Mutation Fuzzing; Optimizing Your Fuzzing Time with Smart Target Selection; Automating Target Monitoring While Fuzzing with Sulley; Leveraging Microsoft Word Macros for Fuzzing .docx files; Block-Based Code Coverage Techniques Using Paimei

SECTION 4: Exploiting Linux for Penetration Testers

Section 4 begins by walking through memory from an exploitation perspective as well as introducing x86 assembler and linking and loading. Processor registers are directly manipulated by testers and must be intimately understood. Disassembly is a critical piece of testing and will be used throughout the remainder of the course. We will take a look at the Linux OS from an exploitation perspective and discuss the topic of privilege escalation.

Topics: Stack and Dynamic Memory Management and Allocation on the Linux OS; Disassembling a Binary and Analyzing x86 Assembly Code; Performing Symbol Resolution on the Linux OS; Identifying Vulnerable Programs; Code Execution Redirection and Memory Leaks; Return-Oriented Programming (ROP); Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Defeating Stack Protection on the Linux OS; Defeating ASLR on the Linux OS

SECTION 5: Exploiting Windows for Penetration Testers

In section 5 we start with covering the OS security features (ALSR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS.

Topics: The State of Windows OS Protections on Windows 7, 8, 10, Server 2008 and 2012; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Using ROP; Building ROP Chains to Defeat DEP and Bypass ASLR; Windows 7 and 8; Porting Metasploit Modules; Client-side Exploitation; Windows Shellcode

SECTION 6: Capture-the-Flag Challenge

This section will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they capture flags. More difficult challenges will be worth more points. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.

> **"Most comprehensive coverage of fuzzing – I would have signed up for the course for that alone."**
>
> — Adam Kliarsky, **Cedars-Sinai Medical Center**

Live Online **sans.org/live-online**

EVENT	START DATE
Security East	Jan 11
Pen Test & Offensive Training	Feb 8
Cyber Security East: Feb	Feb 22
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
SOC Training	Jun 14

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! SEC699: **Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Build a purple team in your organization
- Build realistic adversary emulation plans to better protect your organization
- Develop custom tools and plugins for existing tools to fine-tune your red and purple teaming activities
- Deliver advanced attacks, including application whitelisting bypasses, cross-forest attacks (abusing delegation), and stealth persistence strategies
- Build SIGMA rules to detect advanced adversary techniques

Who Should Attend

- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Red team members
- Blue team members
- Purple team members
- Forensics specialists who want to better understand offensive tactics

Author Statement

"After the success of SEC599, I'm very excited to unleash this course offering upon the SANS audience! SEC699 is an amazing course that came about because we listened to student requests for a hands-on adversary emulation class leveraging an enterprise lab environment. This is it! SEC699 attendees will learn advanced red and blue team techniques for proper purple teaming in an enterprise environment. Throughout the week we do not just focus on explaining "tips and tricks," but also empower students to build and adapt their own tooling for proper adversary emulation. This includes, for example, custom Caldera, SIGMA and Velociraptor development. The SEC699 lab environment is fully built using Ansible playbooks and covers multiple domains and forests that can be attacked! As promised, students will receive the Ansible playbooks AND will acquire the necessary skills to further extend and tailor them for their own custom needs."
— Erik Van Buggenhout

SEC699 is SANS's advanced purple team offering, with a key focus on adversary emulation for data breach prevention and detection. Throughout this course, students will learn how real-life threat actors can be emulated in a realistic, enterprise, environment. In true purple fashion, the goal of the course is to educate students on how adversarial techniques can be emulated and detected.

A natural follow-up to SEC599, this is an advanced SANS course offering, with 60 percent of class time spent on labs. Highlights of class activities include:

- An in-depth course section on how to develop Ansible playbooks that deploy a full multi-domain enterprise environment for adversary emulation at the press of a button.
- Development of custom MITRE Caldera modules for automated adversary emulation. If you truly want to build an emulation pipeline, automation is key!
- Building adversary emulation plans that mimic real-life threat actors such as APT-28, APT-34, and Turla.
- Building a proper process, tooling, and planning for purple teaming
- Cross-forest attacks where students attempt to escalate privileges from their own isolated forest to the common course forest.
- Bypass methods for some common defense techniques (e.g., application whitelisting, Attack Surface Reduction).
- SIGMA rule-building to detect advanced adversary techniques.
- A spectacular capstone that pits red and blue against one another. While red attempts to infiltrate the organization, blue builds a detection capability to detect adversary techniques.

Course authors Erik Van Buggenhout (also the lead author of SEC599) and James Shewmaker (also the lead author of SEC660) are both certified GIAC Security Experts and are hands-on practitioners who have built a deep understanding of how cyber attacks work through both red team (penetration testing) and blue team (incident response, security monitoring, threat hunting) activities. In this course, they combine these skill sets to educate students on adversary emulation methods for data breach prevention and detection.

The SEC699 journey is structured as follows:

- Section 1 will lay the foundations that are required to perform successful adversary emulation and purple teaming. As this is an advanced course, we will go in-depth on several tools that we'll be using and learn how to further extend existing tools.
- Sections 2 to 5 will be heavily hands-on:
  - At the start of each section, we will lecture on an "advanced" technique (e.g., domain delegation attacks)
  - After the initial lecture, we will perform a purple team exercise (both emulation and detection) for a specific threat actor. The advanced technique will be included in the emulation plan
- In Section 6, students will participate in an all-day lab that pits red and blue teams against one another. While red attempts to infiltrate the organization, blue builds a detection capability to detect adversary techniques.

> **"Overall, SEC699 was the best course I've taken as an incident responder and SOC analyst. It simulates the real-world attacks and defending possibilities using numerous kinds of techniques. It provided me with a structure and focus on how to mature our current SOC capabilities."**
>
> — Maurice Von Wintersdorff, **Philips**

SEC699: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Adversary Emulation for Breach Prevention and Detection

In Section 1, we will lay the foundations for the rest of the course by:

- Learning how to build a purple team in-house, covering process, approach, and tooling.
- Leveraging the power of Ansible automation to deploy our lab infrastructure.
- Building an emulation and detection pipeline using a variety of available technology (SIGMA for detection rule development, and various adversary emulation tools, with a focus on Caldera).

Even if it's just the first section, this section is heavily hands-on as students will complete five different exercises.

Topics: Introduction; Course Objectives; Purple Teaming Using MITRE ATT&CK; Purple Team Planning and Follow-up; Automation; Ansible Automation; Building an Emulation and Detection Pipeline; Building a Stack for Detection; Rule-based Versus Anomaly-based Detection; Building a Stack for Adversary Emulation; Automated Emulation Using MITRE Caldera

SECTION 2: Advanced Initial Execution Techniques – Threat Actor APT-28

As indicated in the overall course description: Sections 2 to 5 follow a common structure:

- We will first perform a lecture and stand-alone lab on an advanced adversary technique and how it can be emulated.
- Afterwards, we will build an emulation plan for a specific threat actor. The emulation plan will include the advanced technique covered in the lecture.
- All techniques in the emulation will first be executed manually.
- Upon manual completion of the emulation plan, we will review which steps of the plan could have been detected, and how. We will implement community SIGMA rules, but also develop our own rules to detect the steps of the emulation plan.
- We will proceed by emulating the same plan in Caldera, where we will develop our own ATT&CK techniques as required.
- We will test our implemented SIGMA rules by executing the automated adversary plan.

Topics: Topic for the Day – Advanced Initial Execution; Threat Actor for the Day – APT-28; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated; Conclusion

SECTION 3: Advanced Active Directory Attacks – Threat Actor APT-34

As indicated in the overall course description: Sections 2 to 5 follow a common structure:

- We will first perform a lecture and stand-alone lab on an advanced adversary technique and how it can be emulated.
- Afterwards, we will build an emulation plan for a specific threat actor. The emulation plan will include the advanced technique covered in the lecture.
- All techniques in the emulation will first be executed manually.
- Upon manual completion of the emulation plan, we will review which steps of the plan could have been detected, and how. We will implement community SIGMA rules, but also develop our own rules to detect the steps of the emulation plan.
- We will proceed by emulating the same plan in Caldera, where we will develop our own ATT&CK techniques as required.
- We will test our implemented SIGMA rules by executing the automated adversary plan.

Topics: Topic for the Day – Advanced AD Attacks; Threat Actor for the Day – APT-34; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated; Conclusion

SECTION 4: Stealth Persistence Strategies & Turla

As indicated in the overall course description: Sections 2 to 5 follow a common structure:

- We will first perform a lecture and stand-alone lab on an advanced adversary technique and how it can be emulated.
- Afterwards, we will build an emulation plan for a specific threat actor. The emulation plan will include the advanced technique covered in the lecture.
- All techniques in the emulation will first be executed manually.
- Upon manual completion of the emulation plan, we will review which steps of the plan could have been detected, and how. We will implement community SIGMA rules, but also develop our own rules to detect the steps of the emulation plan.
- We will proceed by emulating the same plan in Caldera, where we will develop our own ATT&CK techniques as required.
- We will test our implemented SIGMA rules by executing the automated adversary plan.

Topics: Topic for the Day – Stealth Persistence; Threat Actor for the Day – Turla; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated; Conclusion

SECTION 5: Azure AD Attacks

As indicated in the overall course description: Sections 2 to 5 follow a common structure:

- We will first perform a lecture and stand-alone lab on an advanced adversary technique and how it can be emulated.
- Afterwards, we will build an emulation plan for a specific threat actor. The emulation plan will include the advanced technique covered in the lecture.
- All techniques in the emulation will first be executed manually.
- Upon manual completion of the emulation plan, we will review which steps of the plan could have been detected, and how. We will implement community SIGMA rules, but also develop our own rules to detect the steps of the emulation plan.
- We will proceed by emulating the same plan in Caldera, where we will develop our own ATT&CK techniques as required.
- We will test our implemented SIGMA rules by executing the automated adversary plan.

Topics: Topic for the Day – Azure AD Attacks; Threat Actor for the Day – APT-30; Implement Detection Use Cases; Execute Adversary Emulation Plan – Automated; Conclusion

SECTION 6: Adversary Emulation Capstone

In this final section of the SEC699 course, participants can choose whether to join the red or blue team in an epic capstone battle to infiltrate or defend the corporate environment. Students will leverage all of the tools and techniques they've learned throughout the course!

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Pen Test & Offensive Training	Feb 8
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19
Purple Team Summit	May 17
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC760: **Advanced Exploit Development for Penetration Testers**

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Discover zero-day vulnerabilities in programs running on fully patched modern operating systems
- Use the advanced features of IDA Pro and write your own IDA Python scripts
- Perform remote debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows
- Write Return-Oriented Shellcode
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows heap overflows and use-after-free attacks
- Perform Windows kernel debugging up through Windows 10 64-bit Build 1903
- Perform Windows driver and kernel exploitation

Vulnerabilities in modern operating systems such as Microsoft Windows 10 and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skill set to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skill set regardless of the increased complexity. SEC760: Advanced Exploit Development for Penetration Testers, the SANS Institute's only 700-level course, teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, kernel and driver exploitation, one-day exploitation through patch analysis, and other advanced attacks
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success

Course Authors' Statements

"As a perpetual student of information security, I am excited to offer SEC760: Advanced Exploit Writing for Penetration Testers. Exploit development is a hot topic as of late and will continue to increase in importance moving forward. With all of the modern exploit mitigation controls offered by operating systems such as Windows 7 and 8, the number of experts with the skills to produce working exploits is highly limited. More and more companies are looking to hire professionals with the ability to conduct a Secure-SDLC process, perform threat modeling, determine if vulnerabilities are exploitable, and carry out security research. This course was written to help you get into these highly sought-after positions and to teach you cutting-edge tricks to thoroughly evaluate a target, providing you with the skills to improve your exploit development."
— Stephen Sims

"Teaching and helping author SEC760: Advanced Exploit Writing for Penetration Testers has given me the opportunity to distill my past experiences in exploit writing and technical systems knowledge into a format worth sharing. This course is meant to give you a look into a number of different exploitation techniques and serves as an amazing jumping-off point for exploitation of any modern application or system. Even if you don't plan on having a career in exploit writing or vulnerability research, this course will be valuable in understanding the thought process that goes into constructing an exploit and what technologies exist to stop an exploit writer from being successful."
— Jaime Geiger

> **"I've taken many other advanced exploit dev classes and none of them break it down and step through the exploits like this class."**
>
> — Adam Logue, **SecureWorks**

> **"SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned."**
>
> — Jenny Kitaichit, **Intel**

SEC760: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Exploit Mitigations and Reversing with IDA

The course starts with a deep dive into both mature and modern exploit mitigations. It is rare today to come across an application or operating system that doesn't use a combination of mitigations to thwart the exploitation of a vulnerability. Outdated operating systems and applications do exist, such as in the industrial control system and Internet of Things space, but that is not the focus of this course. We address the effectiveness and technical details behind each control, such as those implemented in Windows Defender Exploit Guard. We then spend the remainder of Section 1 using IDA Pro, which comes bundled with the course. We quickly ramp up on the basics of IDA Pro as a disassembler and then move into remote debugging with the tool. We finish up Section 1 utilizing IDA FLIRT and FLAIR and writing IDAPython scripts to help with bug hunting and analysis.

Topics: Exploit Mitigations; Windows Defender Exploit Guard; Introduction to IDA Pro; Debugging with IDA Pro; FLIRT & FLAIR; Scripting with IDAPython and Python 3

SECTION 2: Advanced Linux Exploitation

The ability to progress into more advanced reversing and exploitation requires an expert-level understanding of basic software vulnerabilities, such as those covered in SANS' SEC660 course. Heap overflows serve as a rite of passage into modern exploitation techniques. This section is aimed at bridging this gap of knowledge in order to inspire thinking in a more abstract manner, which is necessary to continue further with the course. Linux can sometimes be an easier operating system to learn these techniques, serving as a productive gateway into Windows. Most courses on exploit development focus purely on the Windows OS, and it's important to have an understanding of vulnerability research on the Linux OS as well.

Topics: Linux Heap Management, Constructs, and Environment; Navigating the Heap; Abusing Macros such as unlink() and frontlink(); Function Pointer Overwrites; Format String Exploitation; Abusing Custom Doubly-Linked Lists; Defeating Linux Exploit Mitigation Controls; Using IDA for Linux Application Exploitation; Using Format String Bugs for ASLR Bypass

SECTION 3: Patch Diffing, One-Day Exploits, and Return-Oriented Shellcode

Attackers often download patches as soon as they are distributed by vendors such as Microsoft in order to find newly patched vulnerabilities. Vulnerabilities are usually disclosed privately, or even discovered in-house, allowing the vendor to more silently patch the vulnerability. This also allows the vendor to release limited or even no details at all about a patched vulnerability. Attackers are well aware of this and quickly work to find the patched vulnerability in order to take control of unpatched systems. This technique is also used by incident handlers, IDS administrators and vendors, vulnerability and penetration testing framework companies, government entities, and others. You will use the material covered in this section to identify bugs patched by vendors and take them through to exploitation.

Topics: The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with BinDiff, patchdiff2, turbodiff, and DarunGrim4; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)

SECTION 4: Windows Kernel Debugging and Exploitation

The Windows kernel is complex and intimidating, so this section aims to help you understand the Windows kernel and the various exploit mitigations added into recent versions. You will learn how the kernel works with drivers to talk to devices and how some functionality can be exposed to user-mode, sometimes insecurely! You will perform kernel debugging on Windows 10 and learn to deal with its inherent complexities. Exercises will be performed to analyze Ring 0 driver vulnerabilities, look at exploitation techniques, and get working exploits.

Topics: Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows 10 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HAL Dispatch Table Overwrites

SECTION 5: Advanced Windows Exploitation

The focus of this section is on the advanced exploitation of applications running on the Windows OS. For many years now memory corruption bugs have been the de facto standard regarding exploiting Windows applications. Examples include Use After Free (UAF) and Type Confusion bugs. Many of these vulnerabilities exist due to complexities with large C++ applications such as object tracking and dynamic memory management. In this section we focus on these types of application vulnerabilities on the Windows 7, 8, and 10 operating systems.

Topics: Windows Heap Management, Constructs, and Environment; Understanding the Low Fragmentation Heap (LFH); Browser-based and Client-side Exploitation; Remedial Heap Spraying; Understanding C++ vftable/vtable Behavior; Modern Heap Spraying to Determine Address Predictability; Use-after-free Attacks and Dangling Pointers; Using Custom Flash Objects to Bypass ASLR; Defeating ASLR, DEP, and Other Common Exploit Mitigation Controls

SECTION 6: Capture-the-Flag Challenge

Section 6 will feature a Capture-the-Flag event employing different types of challenges from material taught throughout the week. Test your reverse-engineering, bug discovery, and exploit-writing skills in a full section of Capture-the-Flag exercises!

Who Should Attend

- Senior network and system penetration testers
- Secure application developers (C and C++)
- Reverse-engineering professionals
- Senior incident handlers
- Senior threat analysts
- Vulnerability researchers
- Security researchers

Live Online **sans.org/live-online**

EVENT	START DATE
SANS 2021	Mar 22
Pen Test Austin: Virtual Edition	Apr 19

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! FOR308: **Digital Forensics Essentials**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Effectively use digital forensics methodologies
- Ask the right questions in relation to digital evidence
- Understand how to conduct digital forensics engagements compliant with acceptable practice standards
- Develop and maintain a digital forensics capacity
- Understand incident response processes and procedures and when to call on the team
- Describe potential data recovery options in relation to deleted data
- Identify when digital forensics may be useful and understand how to escalate to an investigator
- If required, use the results of your digital forensics in court

Course Topics

- Introduction to digital investigation and evidence
- Where to find digital evidence
- Digital forensics principles
- Digital forensics and incident response processes
- Digital forensics acquisition
- Digital forensics examination and analysis
- Presenting your findings
- Understanding digital forensic reports
- Challenges in digital forensics
- Building and developing digital forensics capacity
- Legality of digital evidence
- How to testify in court

More than half of jobs in the modern world use a computer. The vast majority of people aged 18-30 are "digitally fluent," accustomed to using smartphones, smart TVs, tablets and home assistants, in addition to laptops and computers, simply as part of everyday life. Yet, how many of these users actually understand what's going on under the hood? Do you know what your computer or smartphone can tell someone about you? Do you know how easy it might be for someone to access and exploit that data? Are you fed up with not understanding what technical people are talking about when it comes to computers and files, data and metadata? Do you know what actually happens when a file is deleted? Do you want to know more about Digital Forensics and Incident Response (DFIR)? If you answered "yes" to any of the above, this course is for you. This is an introductory course aimed at giving people from non-technical backgrounds an understanding, in layman's terms, of how files are stored on a computer or smartphone. It explains what DFIR is and the art of the possible when professionals in these fields are given possession of a device.

This course is intended to be a starting point in the SANS catalogue and provide a grounding in knowledge that other, more in-depth, courses will expand upon.

IT'S NOT JUST ABOUT USING TOOLS AND PUSHING BUTTONS

Digital forensics has evolved from methods and techniques used by detectives in the 1990s to get digital evidence from computers into a complex and comprehensive discipline. The sheer volume of digital devices and data that we could use in investigative ways meant that digital forensics was no longer just being used by police detectives. It was now being used as a full forensic science. It was being used in civil legal processes. It was being used in the military and intelligence services to gather intelligence and actionable data. It was being used to identify how people use and mis-use devices. It was being used to identify how information systems and networks were being compromised and how to better protect them. And that is just some of the current uses of digital forensics.

However digital forensics and incident response are still largely misunderstood outside of a very small and niche community, despite their uses in the much broader commercial, information security, legal, military, intelligence and law enforcement communities.

Many digital forensics and incident response courses focus on the techniques and methods used in these fields, which often do not address the core principles: what digital forensics and incident response are and how to actually make use of digital investigations and digital evidence. This course provides that. It serves to educate the users and potential users of digital forensics and incident response teams so that they better understand what these teams do and how their services can be better leveraged. Users include executives, managers, regulators, legal practitioners, military and intelligence operators and investigators. In addition, not only does this course serve as a foundation for prospective digital forensics practitioners and incident responders, but it also fills in the gaps in fundamental understanding for existing digital forensics practitioners who are looking to take their capabilities to a whole new level.

> **"FOR308 is packed with technical information and covers aspects necessary for those taking their first steps in digital forensics as well as those who think about leading teams in the field. An overall good balance of theory to practice, delivered in a very professional manner."**
>
> — Wiktor Kardacki, **6point5**

FOR308: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Introduction to Digital Investigation

The volume of digital information in the world is growing at a scarily fast rate. In fact, 90 percent of the digital data that exists worldwide today was created within the last two years and it's not slowing down, with 2.5 quintillion bytes of new data created each and every day. If you are investigating any matter, whether it is a crime or an administrative or civil issue, or if you are trying to figure out how your network was compromised, you need evidence. If you are gathering intelligence, you need information. The simple reality is that these days the vast majority of potential evidence or information that we can use, whether it is for investigations, court, or intelligence purposes, is digital in nature. To effectively conduct digital investigations, one needs to understand exactly what digital evidence is, where to find it, the issues affecting it, and the unique challenges it poses. This will allow one to understand the crucial role that digital forensics plays with regard to digital evidence.

Topics: Introduction to Digital Investigation; Digital Forensics Fundamentals; Incident Response Fundamentals Response Fundamentals; Digital Forensics Management

SECTION 3: Incident Response and Digital Forensic Readiness

INCIDENT RESPONSE
Incident Response is the core set of principles and processes necessary to allow an organization to successfully respond, react and remediate against potential attack scenarios.

Topics: Documentation and Reporting in Digital Forensics; Legal Aspects of Digital Forensics; Incident Response Challenges

DIGITAL FORENSICS MANAGEMENT
Good management of a digital forensics or incident response team is key in allowing an organization to successfully respond to potential attack scenarios and investigate digital evidence.

Topics: Introduction to Forensic Readiness; The Need for Forensic Readiness; Building and Managing a DFIR Capacity

SECTION 5: Digital Forensic Analysis

The key purpose of digital forensics is to find answers, and it is through the analysis process that digital forensics transforms raw data into either evidence or intelligence that we can use to answer the questions that we need answered. The use of technology is so integral to our day-to-day activities that it allows us an unprecedented opportunity to reconstruct what has happened in the past, learn what is happening in the present, and even predict what may happen in the future, all based on the data available to us. By understanding digital forensic analysis, we can see how we can ask the right questions in our investigations and intelligence efforts, how we can critically examine and analyze the data at hand in a manner that can withstand scrutiny, and, finally, understand the types of answers we can get.

Topics: What Can Forensic Analysis Prove; Planning the Examination; The Art and Science of Forensic Analysis; Forensic Examination and Analysis Standards; Forensic Examination and Analysis Challenges

SECTION 2: Digital Forensics

Digital forensics is the core set of principles and processes necessary to produce usable digital evidence and uncover critical intelligence. Digital forensics is crucial to ensure accurate and usable digital evidence, but it is important to understand exactly what it is, what it can do, and how it can be used. If you are a user of digital forensics and digital evidence, understanding exactly how digital forensics works will enable you to better make use of digital forensics and digital evidence. If you are a manager or supervisor of a digital forensic team, this will help you understand exactly how it should be functioning and how to build and maintain it. Finally, if you are a prospective digital forensics practitioner or an existing one, this will equip you with the fundamental knowledge and skills that form the core of the digital forensic profession.

Topics: Digital Forensics Management; Digital Evidence Acquisition Essentials; Concepts of Digital Forensic Analysis; Digital Forensics Challenges

SECTION 4: Evidence Acquisition Essentials

Acquiring digital evidence is a crucial component in any investigation. Digital forensics is about finding answers, and if we cannot get to the evidence that we need, which is often stored on devices, in memory, on the wire or wireless, or in the Cloud, then we will never be able to get the answers we seek. Getting the digital evidence and selecting the appropriate method to obtain it can mean the difference between success and failure in an investigation. The acquisition of digital evidence has evolved over the years and the old way of doing it may not always be the best or most effective way of getting it and may actually compromise an investigation. By understanding the various strategies and methods available to acquire digital evidence, we can make informed decisions in a given situation or environment.

Topics: Forensic Acquisition Principles and Standards; Understanding Forensic Images; Forensic Acquisition Processes; Acquisition Challenges

SECTION 6: Documenting and Reporting and Going to Court

DOCUMENTING AND REPORTING IN DIGITAL FORENSICS
It doesn't matter how good your technical skills are, if you are not able to effectively document what you have done and report on your findings in a manner that non-technical people understand, your investigation is on shaky ground.

Topics: Ongoing Documentation; Presenting your Findings

GOING TO COURT
While not all digital forensics matters end up going to court, some do, and when that is the case it is important to at least have some understanding of the law of evidence and going to court.

Topics: Legal Evidence; Testifying in Court

Who Should Attend

- Federal agents and law enforcement officers who want to learn the fundamentals of digital forensics, are starting out in digital forensics, are responsible for managing digital forensics units, or who want to know how digital evidence can be used in investigations and other law enforcement operations
- Digital forensic analysts who want to consolidate and expand their understanding of the fundamentals of digital forensics as a discipline
- Information security professionals who want to understand the fundamentals of digital forensics and how to leverage this in their operational environments
- Legal professionals who need to understand digital forensics, the role it can play in proving a matter in court, the various uses of digital evidence, and the relationship between digital forensics and digital evidence
- Military and intelligence operators who need to understand the role of digital investigation and intelligence gathering, and how digital forensics can enhance their missions
- Human resources professionals who may have to rely on digital forensics and evidence in internal investigations of staff misconduct
- Managers and executives who need to understand what digital forensics can do for their organizations and the critical role that it can play in securing their organization
- Anyone interested in digital forensics, whether or not they are considering a career in this field

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
OSINT Summit	Feb 15
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Security West	May 10
Miami: Virtual Edition	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR498: **Battlefield Forensics & Data Acquisition**

GBFA
Battlefield Forensics and Acquisition
giac.org/gbfa

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where they are stored
- Handle and process a scene properly to maintain evidentiary integrity
- Perform data acquisition from at-rest storage, including both spinning media and solid-state storage
- Identify the numerous places that data for an investigation might exist
- Perform Battlefield Forensics by going from evidence seizure to actionable intelligence in 90 minutes or less
- Assist in preparing the documentation necessary to communicate with online entities such as Google, Facebook, Microsoft, etc.
- Understand the concepts and usage of large-volume storage technologies, including JBOD, RAID storage, NAS devices, and other large-scale, network addressable storage
- Identify and collect user data within large corporate environments where they are accessed using SMB
- Gather volatile data such as a computer system's RAM
- Recover and properly preserve digital evidence on cellular and other portable devices
- Address the proper collection and preservation of data on devices such as Microsoft Surface/Surface Pro, where hard-drive removal is not an option
- Address the proper collection and preservation of data on Apple devices such as MacBook, MacBook Air, and MacBook Pro, where hard-drive removal is not an option
- Properly collect and effectively target email from Exchange servers, avoiding the old-school method of full acquisition and subsequent onerous data culling
- Properly collect data from SharePoint repositories
- Access and acquire online mail stores such as Gmail, Hotmail, and Yahoo Mail accounts

Who Should Attend

- Federal agents and law enforcement personnel
- First responders
- Digital forensic analysts
- Information security professionals
- Incident response team members
- Media exploitation analysts
- Department of Defense and intelligence community professionals
- Anyone interested in an understanding of the proper preservation of systems

THE CLOCK IS TICKING. YOU NEED TO PRIORITIZE THE MOST VALUABLE EVIDENCE FOR PROCESSING. LET US SHOW YOU HOW!

FOR498: Battlefield Forensics & Acquisition will help you to:

- Acquire data effectively from:
  - PCs, Microsoft Surface, and Tablet PCs
  - Apple Devices, and Mac, and Macbooks
  - RAM and memory
  - Smartphones and portable mobile devices
  - Cloud storage and services
  - Network storage repositories
- Produce actionable intelligence in 90 minutes or less

The first step in any investigation is the gathering of evidence. Digital forensic investigations are no different. The evidence used in this type of investigation is data, and this data can live in many varied formats and locations. You must be able to first identify the data that you might need, determine where that data resides, and, finally, formulate a plan and procedures for collecting that data.

With digital forensic acquisitions, you will typically have only one chance to collect data properly. If you manage the acquisition incorrectly, you run the risk of not only damaging the investigation, but more importantly, destroying the very data that could have been used as evidence.

With the wide range of storage media in the marketplace today, any kind of standardized methodology for all media is simply untenable. Many mistakes are being made in digital evidence collection, and this can cause the guilty to go free and, more importantly, the innocent to be incarcerated. The disposition of millions and millions of dollars can rest within the bits and bytes that you are tasked with properly collecting and interpreting.

An examiner can no longer rely on "dead box" imaging of a single hard drive. In today's cyber sphere, many people utilize a desktop, laptop, tablet, and cellular phone within the course of a normal day. Compounding this issue is the expanding use of cloud storage and providers, and the proper collection of data from all these domains can become quite overwhelming.

This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly identify, collect, respond to, and preserve data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach. Constantly updated, FOR498 addresses today's need for widespread knowledge and understanding of the challenges and techniques that investigators require when addressing real-world cases.

Numerous hands-on labs throughout the course will give first responders, investigators, and digital forensics teams the practical experience needed when performing digital acquisition from hard drives, memory sticks, cellular phones, network storage areas, and everything in between.

During a digital forensics response and investigation, an organization needs the most skilled responders possible, lest the investigation end before it has begun. FOR498: Battlefield Forensics & Acquisition will train you and your team to properly handle and make use of data no matter where it hides or resides.

> **"This course presented some useful info that I wasn't aware of previously, i.e., RAID acquisition, tool usage, and data recovery."**
>
> — Nina Turner, **Travelers**

FOR498: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Evidence File Quick Wins and Dealing with Smartphones

Investigators will often be responding in high-stress environments where many different entities are critically scrutinizing the collection process. Personnel need to be properly trained and equipped to work in less than optimal surroundings, and be confident that they have managed the scene, identified all necessary data, collected the data in a properly defensible manner, and maintained its integrity. One of the most common scenarios that can cause headaches is receiving an evidence file (usually an E01), and being expected to provide answers immediately. The common approach is to mount the image and then start running carving and other tools against it. These automated tasks can take many hours (and sometimes days) just by themselves! Portable devices bring their own set of challenges to the table. These devices are more ubiquitous than computers. Seldom is the case today that does not include a cellular device. Unfortunately, there is no standard for the cellular operating systems. Even within brands, there can be vastly different data storage. Today will introduce the student to several devices and the tools that will acquire them.

Topics: SIFT Introduction; Introduction to Digital Forensic Acquisition; Understanding the Data; Smartphone Acquisition; Smartphone Analysis; Android

SECTION 2: Evidence Acquisition and Collection

Investigators and first responders should be armed with the latest tools, digital container access techniques, and enterprise methodologies to identify, access, and preserve evidence across a vast range of devices and repositories. Personnel must also be able to scale their identification and collection across thousands of systems in their enterprise. Enterprise and cloud storage collection techniques are now a requirement to track activity that has been intentionally and unintentionally spread across many devices. Responding to these many systems cannot be accomplished using the standard "pull the hard drive" forensic examination methodology. Such an approach will cause frustration and result in lost opportunities due to the time it takes to forensically image entire hard drives. Furthermore, investigators need actionable intelligence as quickly and responsibly as possible. This section lays the foundation for evidence collection, from initial arrival on a scene to the fundamentals of understanding data at rest and properly identifying devices, interfaces, and tools that will be necessary to affect a successful collection. This course section will explore the myriad of acquisition hardware and software, not to mention adapters and identification, so we can make the best decisions about the data.

Topics: Scene Management and Evidence Acquisition; Device and Interface Identification; Acquisition Hardware and Software; Acquisition Methodology; Discovering and Interacting with Data

SECTION 3: Quick Win Forensics

Given that 99% of the necessary evidence typically will exist in 1-2% of the data acquired, it is easy to see how a great deal of time can be wasted following the normal procedures in today's digital forensics world. Instead, let's focus on this 1-2% and perform a very rapid triage collection that can be used to start our investigation sooner! Far too often, computers are seized in an "on" state, and immediately powered down because, "that is how we've always done it." With today's computers this means you are throwing away (essentially destroying) many gigabytes of data. The RAM in a computer holds an incredibly important treasure trove of data, from keystrokes to network connections, running services, and, quite importantly, passwords and decryption keys. With the vastly increasing spread of file-less malware, in many cases the only place that evidence will exist is in memory. Another often-overlooked factor is full disk encryption. In cases like this, "live" acquisition will be your only hope.

Topics: Beginning the Collection Process; Mounting Evidence; Triage Acquisition; Memory Acquisition and Encryption; Host-based Live Acquisition Checking

SECTION 4: Non-Traditional and Cloud Acquisition

When we think about acquisition, it usually involves opening the side of the computer, removing the hard drive, connecting to a write blocker or imaging equipment, and completing the task. While this is not an inaccurate assessment, it does not address a great deal of the access and acquisition questions surrounding so much data today. If full disk imaging is necessary, then it is certainly easier and quicker to do it directly from the storage itself. But what happens with devices such as iPads, Surface Books, and other such equipment, where it is glue and not screws that hold them together? Volume Shadow Copies also contain a wealth of historic data that is of great use to investigators. Knowing how to access and collect data from these shadow copies is critical in cases involving the Windows operating system. Battlefield forensics is considered the bleeding edge of digital forensics. It requires in-depth knowledge of where the most valuable data resides on the computer and how to get at it as fast as possible. An effective battlefield forensicator needs to be extracting actionable intelligence in 90 minutes or less, but the clock does not start when the forensic imaging is done. Rather. it starts from the moment you lay your hands on the device. Learn how to identify and access data in non-traditional storage areas. In today's world so much data lives off site, and there are very few methods in place to access and properly acquire it. In this section, we will identify these locations, including SharePoint, Exchange, webmail, network locations, cloud storage, and social media, not to mention Dropbox, Google Drive, and the Internet of Things. This also includes RAID storage and how to best collect these devices regardless of configuration.

Topics: Dead Box Acquisition; File Systems Revisited; Battlefield Forensics with KAPE; Multi-Drive Storage; EMC/Non-traditional Formats; Remote Acquisition

SECTION 5: Apple Acquisition, Internet of Things, and Online Attribution

There are very few tools and techniques available when it comes to acquisition of Apple products, as compared to Windows. The tools that exist can be quite expensive, and free tools are simply few and far between. In this section, we will explore the fundamentals of acquiring data from Apple devices. We will acquire memory and identify systems that are running CoreStorage technology and full disk encryption. We will also visit the challenges posed by APFS. Many of the Apple systems are closed systems, in that you simply cannot remove the hard drive, as it is soldered directly to the motherboard. The uniqueness of the data storage demands alternative methods of acquisition. In this course section, you'll learn how to access and forensically image iPads, MacBooks, and other HFS+ devices, working at the command line. You have traced an artifact back to an IP, email, or web address. Now what? We will learn the best methods for determining attribution, from proper collection to legal documentation. Not to be left out, the Internet of Things is pervasive. It is controlling our fridges, thermostats, security cameras, and door locks. It is listening passively and waiting patiently for an instruction to perform. Today you will learn how these devices communicate, and more importantly, who is controlling them.

Topics: Identifying Online Asset Ownership; Apple MacOS Device Overview and Acquisition; Internet of Things

SECTION 6: Beyond the Forensic Tools: The Deeper Dive

The usefulness of file and stream carving cannot be overstated. Some data simply do not live in the defined file space that can be readily accessed by a viewer. From partially overwritten to deleted data, we will explore techniques you can employ when traditional tools fail. Data carving is a skill that is increasingly important. Once the reference to a file is destroyed, how can the data still be recovered? File carving tools will assist in this, but examiners must understand the limitations of their tools. Without the proper pieces of the original file, a carver is useless. At some point, you will be faced with non-functioning media. Learn about the inner workings of hard drives, and what you can (and cannot) do to revive them to a point where you can then create your forensic image. We will also be looking at the "best of breed" data recovery tools, from those that are free to those that cost many thousands of dollars.

Topics: File and Stream Recovery; Advanced Data Carving and Rebuilding; Data Recovery; Where Do We Go From Here

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security West: Feb	Feb 1
Cyber Security East: March	Mar 1
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
DFIRCON Spring	May 3
Miami: Virtual Edition	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR500: **Windows Forensic Analysis**

GCFE
Forensic Examiner
giac.org/gcfe

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7, Windows 8/8.1, and Windows10
- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), email analysis, and Windows Registry parsing
- Audit cloud storage usage, including detailed user activity, identifying deleted files, and even documenting files available only in the cloud
- Identify keywords searched by a specific user on a Windows system to pinpoint the data and information that the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows Shellbag analysis tools to articulate every folder and directory that a user or attacker opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing Windows artifacts such as the Registry and Event Log files
- Learn Event Log analysis techniques and use them to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

FOR500: Windows Forensic Analysis will teach you to:

- Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012/2016
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation experts capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. You will learn how to recover, analyze, and authenticate forensic data on Windows systems, track particular user activity on your network, and organize findings for use in incident response, internal investigations, and civil/criminal litigation. You will be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, Cloud Storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. The course starts with an intellectual property theft and corporate espionage case that took over six months to create. You work in the real world, so your training should include real-world practice data. The instructors on our course development team used incidents from their own investigations and experiences to create an incredibly rich and detailed scenario designed to immerse students in an actual investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The detailed workbook shows step-by-step the tools and techniques that each investigator should employ to solve a forensic case.

> **"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."**
>
> — Alexander Applegate, **Auburn University**

FOR500: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Windows Digital Forensics and Advanced Data Triage

The Windows Forensic Analysis course starts with an examination of digital forensics in today's interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. Hard drive sizes are increasingly difficult to handle appropriately in digital cases. Being able to acquire data in an efficient and forensically sound manner is crucial to every investigator today. Most fundamental analysts can easily image a hard drive using a write blocker. In this course, we will review the core techniques while introducing new triage-based acquisition and extraction capabilities that will increase the speed and efficiency of the acquisition process. We will demonstrate how to acquire memory, the NTFS MFT, Windows logs, Registry, and critical files that will take minutes to acquire instead of the hours or days currently spent on acquisition.

Topics: Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

SECTION 2: Core Windows Forensics Part 1 – Windows Registry Forensics and Analysis

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user profile data and system data. The course teaches forensic investigators how to prove that a specific user performed keyword searches, executed specific programs, opened and saved files, perused folders, and used removable devices. Data is moving rapidly to the cloud, constituting a significant challenge and risk to the modern enterprise. Cloud storage applications are nearly ubiquitous on both consumer and business systems, causing interesting security and forensic challenges. In a world where some of the most important data is only present on third-party systems, how do we effectively accomplish our investigations? In this section we will dissect OneDrive, Google Drive, G Suite, Dropbox, and Box applications, deriving artifacts present in application logs and left behind on the endpoint. Detailed user activity, history of deleted files and discovery of cloud contents are all possible. Solutions to the very real challenges of forensic acquisition are also discussed. Understanding what can be gained through analysis of these popular applications will make investigations of less common cloud storage solutions easier when encountered.

Topics: Registry Core; Profile Users and Groups; Core System Information; User Forensic Data; Cloud Storage Forensics; Tools Used

SECTION 3: Core Windows Forensics Part 2 – USB Devices and Shell Items

Being able to show the first and last time a file or folder was opened is a critical analysis skill. Utilizing shortcut (LNK), jump list, and Shellbag databases through the examination of SHELL ITEMS, we can quickly pinpoint which file or folder was opened and when. The knowledge obtained by examining SHELL ITEMS is crucial in tracking user activity in intellectual property theft cases internally or in tracking hackers. Removable storage device investigations are often an essential part of performing digital forensics. We will show you how to perform in-depth USB device examinations on Windows 7, 8/8.1, and 10. You will learn how to determine when a storage device was first and last plugged in, its vendor/make/model, and even the unique serial number of the device used.

Topics: Shell Item Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations

SECTION 4: Core Windows Forensics Part 3 – Email, Key Additional Artifacts, and Event Logs

Depending on the type of investigation and authorization, a wealth of evidence can be unearthed through the analysis of email files. Recovered email can bring excellent corroborating information to an investigation, and its informality often provides very incriminating evidence. It is common for users to have an email that exists locally on their workstation, on their company email server, in a private cloud, and in multiple webmail accounts. Additional artifacts such as Windows Prefetch are paramount to proving evidence of execution. The exciting Windows 10 Timeline database shows great promise in recording detailed user activity. Similarly, the System Resource Usage Monitor (SRUM), one of our most exciting digital artifacts, can help determine several important user actions, including network usage by cloud storage and backdoors, even after execution of counter-forensic programs. Finally, Windows event log analysis has solved more cases than possibly any other type of analysis. Understanding the locations and content of these files is crucial to the success of any investigator. Many researchers overlook these records because they do not have adequate knowledge or tools to get the job done efficiently. This section arms each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

Topics: Email Forensics; Forensicating Additional Windows OS Artifacts; Windows Event Log Analysis

SECTION 5: Core Windows Forensics Part 4 – Web Browser Forensics for Firefox, Internet Explorer, and Chrome

With the increasing use of the web and the shift toward web-based applications and cloud computing, browser forensic analysis is a critical skill. During this section, the investigator will comprehensively explore web browser evidence created during the use of Internet Explorer, Edge, Firefox, and Google Chrome. The hands-on skills taught here, such as SQLite and ESE database parsing, allow investigators to extend these methods to nearly any browser they encounter. The analyst will learn how to examine every significant artifact stored by the browser, including cookies, visit and download history, Internet cache files, browser extensions, and form data. We will show you how to find these records and identify the common mistakes investigators make when interpreting browser artifacts. You will also learn how to analyze some of the more obscure (and powerful) browser artifacts, such as session restore, tracking cookies, zoom levels, predictive site prefetching, and private browsing remnants. Finally, browser synchronization is explored, providing investigative artifacts derived from other devices. Throughout the section, investigators will use their skills in real hands-on cases, exploring evidence created by Chrome, Firefox, Edge, Internet Explorer, and Tor correlated with other Windows operating system artifacts.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding Browser Timestamps, Internet Explorer; Edge; Firefox; Chrome; Examining of Browser Artifacts; Tools Used

SECTION 6: Windows Forensic Challenge

Nothing will prepare you more as an investigator than a full hands-on challenge that requires you to use the skills and knowledge presented throughout the course. At the start of this section, you will have the option to work in teams on a real forensic case. Students will be provided new evidence to analyze, and the exercise will step you through the entire case flow, including proper acquisition, analysis, and reporting in preparation for a possible trial. Teams will work on the case with the objective of profiling computer usage and discovering the most critical pieces of evidence to present. This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections. The section will conclude with a mock trial involving presentations of the evidence collected. The team with the best in-class presentation and short write-up wins the challenge...and the case!

Topics: Digital Forensic Case; Presentation

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
Cyber Security West: Feb	Feb 1
Cyber Security East: March	Mar 1
Cyber Security West: March	Mar 15
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Rocky Mountain Spring	Apr 26
DFIRCON Spring	May 3
Security West	May 10
Cyber Security Central: June	Jun 7
Miami: Virtual Edition	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR508: **Advanced Incident Response, Threat Hunting, and Digital Forensics**

GCFA
Forensic Analyst
giac.org/gcfa

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection
- Understand how the attacker can acquire legitimate credentials – including domain administrator rights – even in a locked-down environment

Who Should Attend

- Incident response team members
- Threat hunters
- Security Operations Center analysts
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates

ADVANCED THREATS ARE IN YOUR NETWORK – IT'S TIME TO GO HUNTING!

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done significant damage to the organization. For the incident responder, this process is known as "threat hunting," which uses known adversary behaviors to proactively examine the network and endpoints in order to identify new data breaches.

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

> **"FOR508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can't get any better!"**
>
> — Neel Mehta, **Chevron**

FOR508: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Advanced Incident Response and Threat Hunting

Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to incident response for advanced threat groups. We will show the importance of developing cyber threat intelligence to impact the adversaries' "kill chain". We will also demonstrate live response techniques and tactics that can be applied to a single system and across the entire enterprise.

Topics: Real Incident Response Tactics; Threat Hunting; Threat Hunting in the Enterprise; Incident Response and Hunting across Endpoints; Malware Defense Evasion and Identification; Malware Persistence Identification; Investigating WMI-Based Attacks

SECTION 2: Intrusion Analysis

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. As an example, at some point attackers will need to run code to accomplish their objectives. We can identify this activity via application execution artifacts. Attackers will also need one or more accounts to run code. Consequently, account auditing is a powerful means of identifying malicious actions. Attackers also need a means to move throughout the network, so we look for artifacts left by the relatively small number of ways there are to accomplish this part of their mission. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

Topics: Stealing and Utilization of Legitimate Credentials; Advanced Evidence of Execution Detection; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Log Analysis for Incident Responders and Hunters

SECTION 3: Memory Forensics in Incident Response and Threat Hunting

Now a critical component of many incident response and threat hunting teams that regularly detect advanced adversaries in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, PowerShell, and advanced malware used by APT attackers. In fact, some attacks may be nearly impossible to unravel without memory analysis. Memory analysis was traditionally the domain of Windows internals experts, but the recent development of new tools and techniques makes it accessible today to all investigators, incident responders, and threat hunters. Better tools, interfaces and detection heuristics have greatly leveled the playing field. Understanding attack patterns in memory is a core analyst skill applicable across a wide range of endpoint detection and response products. This extremely popular section will cover many of the most powerful memory analysis capabilities available and give you a solid foundation of advanced memory forensic skills to super-charge investigations, regardless of the toolset employed.

Topics: Remote and Enterprise Incident Response; Triage and Enpoint Detection and Reponse; Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

SECTION 4: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. Temporal data are located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. Pioneered by Rob Lee in 2001, timeline analysis has become a critical incident response, hunting, and forensics technique. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time-based artifacts. The analysis that once took days now takes minutes. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

Topics: Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation and Analysis; Super Timeline Creation and Analysis

SECTION 5: Incident Response & Hunting Across the Enterprise – Advanced Adversary and Anti-Forensics Detection

Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. This advanced session will demonstrate techniques used by first responders to identify malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

Topics: Cyber Threat Intelligence; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

SECTION 6: The APT Threat Group Incident Response Challenge

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the course and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hactivist groups.

Topics: Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
CTI Summit	Jan 25
Cyber Security West: Feb	Feb 1
Scottsdale: Virtual Edition	Feb 22
Cyber Security West: March	Mar 15
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
Baltimore Spring: Virtual Edition	Apr 26
DFIRCON Spring	May 3
Security West	May 10
Cyber Security Central: June	Jun 7
Miami: Virtual Edition	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR518: Mac and iOS Forensic Analysis and Incident Response

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals' usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

FORENSICATE DIFFERENTLY!

Digital forensic and incident response investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms. Dealing with these devices as an investigator is no longer a niche skill – every analyst must have the core skills necessary to investigate the Apple devices they encounter.

The constantly updated FOR518: Mac and iOS Forensic Analysis and Incident Response course provides the techniques and skills necessary to take on any Mac or iOS case without hesitation. The intense hands-on forensic analysis and incident response skills taught in the course will enable analysts to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices.

Forensicate Differently!

This course will teach you:

- Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) and Apple File System (APFS) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- User Activity: How to understand and profile users through their data files and preference configurations.
- Advanced Intrusion Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Apple Technologies: How to understand and analyze many Mac and iOS-specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac and iOS Forensic Analysis and Incident Response aims to train a well-rounded investigator by diving deep into forensic and intrusion analysis of Mac and iOS. The course focuses on topics such as the HFS+ and APFS file systems, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who completes this course will have the skills needed to take on a Mac or iOS forensics case.

> **"This course provides good, clear training on Mac OS/iOS and how they relate/differ in several aspects. It's a must for anyone carrying out forensic analysis today."**
>
> — Iain Spence, **MOD**

FOR518: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Mac and iOS Essentials

This section introduces the student to Mac and iOS essentials such as acquisition, timestamps, logical file system, and disk structure. Acquisition fundamentals are the same with Mac and iOS devices, but there are a few tips and tricks that can be used to successfully and easily collect Mac and iOS systems for analysis. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system – the data are the same, only the format differs.

Topics: Apple Essentials; Mac Essentials and Acquisition; iOS Essentials and iOS Acquisition; Disks & Partitions

SECTION 2: File Systems & System Triage

The building blocks of Mac and iOS forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, students will learn the basic principles of the primary file system implemented on MacOS systems. The students will then use that information to look at a variety of great artifacts that use the file system and that are different from other operating systems students have seen in the past. Rounding out the section, students will review Mac and iOS triage data.

Topics: File Systems; Extended Attributes; File System Events Store Database; Spotlight; Mac and iOS Triage; Most Recently Used (MRUs)

SECTION 3: User Data, System Configuration, and Log Analysis

This section contains a wide array of information that can be used to profile and understand how individuals use their computers. The logical Mac file system is made up of four domains: User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations. The System and Local Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This section details basic system information, GUI preferences, and system application data. A basic analysis of system logs can give a good understanding of how a system was used or abused. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.

Topics: User Data and System Configuration; Log Parsing and Analysis; Timeline Analysis and Data Correlation

SECTION 4: Application Data Analysis

In addition to all the configuration and preference information found in the User Domain, the user can interact with a variety of native Apple applications, including the Internet, email, communication, photos, locational data, etc. These data can provide analysts with the who, what, where, why, and how for any investigation. This section will explore the various databases and other files where data are being stored. The student will be able to parse this information by hand without the help of a commercial tool parser.

Topics: Application Permissions; Native Application Fundamentals; Safari Browser; Apple Mail; Communication; Calendar and Reminders; Contacts; Notes; Photos; Maps; Location Data; Apple Watch; Third-Party Apps

SECTION 5: Advanced Analysis Topics

Mac systems implement some technologies that are available only to those with Mac and iOS devices. These include data backup with Time Machine, Document Versions, and iCloud; and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, live response, Mac intrusion and malware analysis, and Mac memory analysis.

Topics: Time Machine; Document Versions; iCloud; Malware and Intrusion Analysis; Live Response; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

SECTION 6: Mac Forensics & Incident Response Challenge

In this final course section, students will put their new Mac forensic skills to the test by running through a real-life scenario with team members.

Topics: In-Depth File System Examination; File System Timeline Analysis; Advanced Computer Forensics Methodology; Mac Memory Analysis; File System Data Analysis; Metadata Analysis; Recovering Key Mac Files; Volume and Disk Image Analysis; Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault; Advanced Log Analysis and Correlation; iDevice Analysis and iOS Artifacts

> **"We have a primarily Mac OS environment and I don't think I could find a tenth of this information through my own research."**
>
> — Kevin Neely, **Pure Storage**

Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, and detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents and/or intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR500, FOR508, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

Live Online sans.org/live-online

EVENT	START DATE
SANS 2021	Mar 22
DFIRCON Spring	May 3

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

GNFA
Network Forensic Analyst
giac.org/gnfa

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing for follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing for accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone lab, modeled after real-world nation-state intrusions and threat actors

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking a perpetrator's network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572 was designed to cover the most critical skills needed for the increased focus on network communications and artifacts in today's investigative work, including numerous use cases. Many investigative teams are incorporating proactive threat hunting into their skills. This involves using existing evidence along with newly-acquired threat intelligence to uncover evidence of previously-unidentified incidents. Other teams focus on post-incident investigations and reporting. Still others engage with an adversary in real time, seeking to contain and eradicate the attacker from the victim's environment. In these situations and more, the artifacts left behind from attackers' communications can provide an invaluable view into their intent, capabilities, successes, and failures.

In FOR572, we focus on the knowledge necessary to examine and characterize communications that have occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap-based dissection, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is under way.

FOR572 is truly an advanced course – we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, full-stake networking knowledge (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between. They will all benefit you throughout the course material as you fight crime.

UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME.

> **"I feel like the last week has been a massive eye-opener into what extra info I can now use in my forensic investigations."**
>
> — Will Barton, **EMSOU**

FOR572: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Off the Disk and Onto the Wire

Although many fundamental network forensic concepts align with those of any other digital forensic investigation, the network presents many nuances that require special attention. In this section you will learn how to apply what you already know about digital forensics and incident response to network-based evidence. You will also become acclimated to the basic tools of the trade.

Topics: Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

SECTION 3: NetFlow and File Access Protocols

Network connection logging, commonly called NetFlow, may be the single most valuable source of evidence in network investigations. Many organizations have extensive archives of flow data due to its minimal storage requirements. Since NetFlow does not capture any content of the transmission, many legal issues with long-term retention are mitigated. Even without content, NetFlow provides an excellent means of guiding an investigation and characterizing an adversary's activities from pre-attack through operations. Whether within a victim's environment or for data exfiltration, adversaries must move their quarry around through the use of various file access protocols. By knowing some of the more common file access and transfer protocols, a forensicator can quickly identify an attacker's theft actions.

Topics: NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol (FTP); Microsoft Protocols

SECTION 5: Encryption, Protocol Reversing, OPSEC, and Intel

Advancements in common technology have made it easier to be a bad guy and harder for us to track them. Strong encryption methods are readily available and custom protocols are easy to develop and employ. Despite this, there are still weaknesses even in the most advanced adversaries' methods. As we learn what the attackers have deliberately hidden from us, we must operate carefully to avoid tipping our hats regarding the investigative progress – otherwise the attacker can quickly pivot, nullifying our progress.

Topics: Encoding, Encryption, and SSL/TLS; Meddler-in-the-Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

SECTION 2: Core Protocols & Log Aggregation/Analysis

There are countless network protocols that may be in use in a production network environment. We will cover those that are most likely to benefit the forensicator in typical casework, as well as several that help demonstrate analysis methods useful when facing new, undocumented, or proprietary protocols. By learning the "typical" behaviors of these protocols, we can more readily identify anomalies that may suggest misuse of the protocol for nefarious purposes. These protocol artifacts and anomalies can be profiled through direct traffic analysis as well as through the log evidence created by systems that have control or visibility of that traffic. While this affords the investigator with vast opportunities to analyze the network traffic, efficient analysis of large quantities of source data generally requires tools and methods designed to scale.

Topics: Hypertext Transfer Protocol (HTTP): Protocol and Logs; Domain Name Service (DNS): Protocol and Logs; Forensic Network Security Monitoring; Logging Protocol and Aggregation; Syslog; Microsoft Eventing; Log Data Collection, Aggregation, and Analysis; Elastic Stack and the SOF-ELK Platform; Basics and Pros/Cons of the Elastic Stack; SOF-ELK

SECTION 4: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools are a mainstay in the network forensicator's toolkit. We'll explore the various roles that commercial tools generally fill, as well as how they can be best integrated into an investigative workflow. With the runaway adoption of wireless networking, investigators must also be prepared to address the unique challenges this technology brings to the table. However, regardless of the protocol being examined or the budget used to perform the analysis, having a means of exploring full-packet capture is a necessity, and having a toolkit to perform this at scale is critical.

Topics: Simple Mail Transfer Protocol (SMTP); Object Extraction with NetworkMiner; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

SECTION 6: Network Forensics Capstone Challenge

This section will combine all of what you have learned prior to and during the course. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

Topics: Network Forensic Case

> **"The exposure to top-notch instruction, relevant information, and hands-on activities (labs) provides a comprehensive learning experience."**
>
> — Ryan Paros

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

Live Online **sans.org/live-online**

EVENT	START DATE
Security East	Jan 11
CTI Summit	Jan 25
Scottsdale: Virtual Edition	Feb 22
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
DFIRCON Spring	May 3
Security West	May 10
Cyber Security Central: June	Jun 7
Miami: Virtual Edition	Jun 21

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR578: **Cyber Threat Intelligence**

GCTI
Cyber Threat Intelligence
giac.org/gcti

6 Day Program	36 CPEs	Laptop Required

Who Should Attend

- Security practitioners should attend because this course is a perfect match with any security skill set, from red teamers to incident responders and is focused on analysis skills.
- Cyber threat intelligence analysts who are looking to formalize their profession and take their analytical skills to the next level.
- Incident response team members who respond to complex security incidents/intrusions and need to know how to detect, investigate, remediate, and recover from compromised systems across an enterprise.
- Threat hunters who are seeking to understand threats more fully and how to learn from them to be able to more effectively hunt threats and counter the tradecraft behind them.
- Security Operations Center personnel and information security practitioners who support hunting operations that seek to identify attackers in their network environments.
- Digital forensic analysts and malware analysts who want to consolidate and expand their understanding of filesystem forensics, investigations of technically advanced adversaries, incident response tactics, and advanced intrusion investigations.
- Federal agents and law enforcement officials who want to master advanced intrusion investigations and incident response, as well as expand their investigative skills beyond traditional host-based digital forensics.
- Technical managers who are looking to build intelligence teams or leverage intelligence in their organizations building off of their technical skillsets.
- SANS alumni looking to take their analytical skills to the next level.

> **"This course provides great value as it focuses on collection of data and modeling and how to use frameworks to build out capabilities."**
>
> — Aaron Bostwick, **General Atomics**

There is no teacher but the enemy!

Every security practitioner should attend the FOR578: Cyber Threat Intelligence course. This course is unlike any other technical training you have experienced. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn the different sources to collect adversary data and how to exploit and pivot off of it
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques that will complement their existing knowledge as well as establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary's intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated threats. Malware is an adversary's tool, but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries' methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organization with the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats.

FOR578: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Cyber Threat Intelligence and Requirements

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word "cyber" entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. It also focuses on getting your intelligence program off to the right start with planning, direction, and the generation of intelligence requirements. As with all sections, this one includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

Topics: Case Study: Carbanak, The Great Bank Robbery; Understanding Intelligence; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

SECTION 3: Collection Sources

Cyber Threat Intelligence analysts must be able to interrogate and fully understand their collection sources. Analysts do not have to be malware reverse engineers, as an example, but they must at least understand that work and know what data can be sought. This section continues from the previous one in identifying key collection sources for analysts. There is also a lot of available information on what is commonly referred to as open-source intelligence (OSINT). In this course section, students will learn to seek and exploit information from Domains, External Datasets, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more while also structuring the data to be exploited for purposes of sharing internally and externally.

Topics: Case Study: Axiom; Collection Source: Domains; Case Study: GlassRAT; Collection Source: External Datasets; Collection Source: TLS Certificates; Case Study: Trickbots; Exploitation: Storing and Structuring Data

SECTION 5: Higher-Order Analysis and Attribution

A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. The skills required to think critically are exceptionally important and can have an organization-wide or national-level impact. In this course section, students will learn about logical fallacies and cognitive biases as well as how to defeat them. They will also learn about nation-state attribution, including when it can be of value and when it is merely a distraction. Students will also learn about nation-state-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations once they complete the course.

Topics: Logical Fallacies and Cognitive Biases; Dissemination: Strategic Case Study: Stuxnet; Fine-Tuning Analysis; Case Study: Sofacy; Attribution

SECTION 2: The Fundamental Skill Set: Intrusion Analysis

Intrusion analysis is at the heart of threat intelligence. It is a fundamental skill set for any security practitioner who wants to use a more complete approach to addressing security. Two of the most commonly used models for assessing adversary intrusions are the "kill chain" and the "Diamond Model." These models serve as a framework and structured scheme for analyzing intrusions and extracting patterns such as adversary behaviors and malicious indicators. In this section students will participate in and be walked through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process in terms of structuring and defining adversary campaigns.

Topics: Primary Collection Source: Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware

SECTION 4: Analysis and Dissemination of Intelligence

Many organizations seek to share intelligence but often fail to understand its value, its limitations, and the right formats to choose for each audience. Additionally, indicators and information shared without analysis are not intelligence. Structured analytical techniques such as the Analysis of Competing Hypotheses can help add considerable value to intelligence before it is disseminated. This section will focus on identifying both open-source and professional tools that are available for students as well as on sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. Students will gain hands-on experience with STIX and understand the CybOX and TAXII frameworks for sharing information between organizations. Finally, the section will focus on building the singular intrusions into campaigns and being able to communicate about those campaigns.

Topics: Analysis: Exploring Hypotheses; Analysis: Building Campaigns; Dissemination: Tactical; Case Study: Sony Attack; Dissemination: Operational

SECTION 6: Capstone: Satisfying Intelligence Requirements Across the Organization

The FOR578 capstone focuses on analysis. Students will be placed on teams, given outputs of technical tools and cases, and work to piece together the relevant information from a single intrusion that enables them to unravel a broader campaign. Students will get practical experience satisfying intelligence requirements ranging from helping the incident response team to satisfying state-level attribution goals. This analytical process will put the students' minds to the test instead of placing a heavy emphasis on using technical tools. At the end of the section, the teams will present their analyses on the multi-campaign threat they have uncovered.

> **"Threat intelligence analysis has been an art for too long, now it can finally become a science at SANS. Mike Cloppert and Robert M. Lee are the industry 'greybeards' who have seen it all. They are the thought-leaders who should be shaping practitioners for years to come."**
>
> — Rich Barger, **ThreatConnect**

> **"This course gives a very smart and structured approach to Cyber Threat Intelligence, something that the global community has been lacking to date."**
>
> — John Geary, **Citigroup**

Live Online **sans.org/live-online**

EVENT	START DATE
CTI Summit	Jan 25
OSINT Summit	Feb 15
Cyber Security West: March	Mar 15
Cyber Security East: April	Apr 12
DFIRCON Spring	May 3
Miami: Virtual Edition	Jun 21

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR585: **Smartphone Forensic Analysis In-Depth**

GASF
Advanced Smartphone Forensics
giac.org/gasf

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device – we'll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes

> **"Really useful to know the differences in the tools used and how to explore and analyze the data in a safe environment."**
>
> — Nageen Mirza, **Deloitte**

FOR585: Smartphone Forensic Analysis In-Depth will help you understand:

- Where key evidence is located on a smartphone
- How the data got onto the smartphone
- How to recover deleted mobile device data that forensic tools miss
- How to decode evidence stored in third-party applications
- How to detect, decompile, and analyze mobile malware and spyware
- Advanced acquisition terminology and free techniques to gain access to data on smartphones
- How to handle locked or encrypted devices, applications, and containers

SMARTPHONES HAVE MINDS OF THEIR OWN. DON'T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE, SUGGESTIONS, OR APPLICATION ASSOCIATIONS AS USER ACTIVITY. IT'S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Smartphone Forensic Analysis In-Depth will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data are saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examination and interpretation of the data is your job and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

FOR585 features 31 hands-on labs, a forensic challenge, and a bonus take-home case that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

This intensive course is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, acquisition shortfalls, extraction techniques (jailbreaks and roots) and encryption. FOR585 offers the most unique and current instruction on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you're working on the day you get back to work.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's time for the good guys to get smarter and for the bad guys to know that their smartphone activity can and will be used against them!

SMARTPHONE DATA CAN'T HIDE FOREVER – IT'S TIME TO OUTSMART THE MOBILE DEVICE!

FOR585: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Smartphone Overview, Fundamentals of Analysis, SQLite Introduction, Android Forensics Overview, and Android Backups

Although smartphone forensic concepts are similar to those of digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. In this first course section, students will apply what they know to smartphone forensic handling, device capabilities, acquisition methods, SQLite database examination, and query development. They'll also gain an overview of Android devices. We end this section by examining Android backups and cloud data associated with Android and Google. Students will become familiar with the most popular forensic tools required to complete comprehensive examinations of smartphone data structures.

Topics: The SIFT Workstation; Introduction to Smartphones; Smartphone Handling; Forensic Acquisition Concepts of Smartphones; Smartphone Components; Smartphone Forensic Tool Overview – Physical Analyzer; Smartphone Forensic Tool Overview – AXIOM; Introduction to SQLite; Android Forensic Overview; Android Backup Files; Google Cloud Data and Extractions

SECTION 3: iOS Device Forensics

Apple iOS devices contain substantial amounts of data (including deleted records) that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed to bypass locked iOS devices and correctly interpret the data. This course section will cover extraction techniques using jailbreaks and exploits. Without iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

Topics: iOS Forensic Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

SECTION 5: Third-Party Application Analysis

This course section starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. The rest of the section focuses heavily on secure chat applications, recovery of deleted application data and attachments, mobile browser artifacts, and knock-off phone forensics. The skills learned in this section will provide students with advanced methods for decoding data stored in third-party applications across all smartphones. We will show you what the commercial tools miss and teach you how to recover these artifacts yourself.

Topics: Third-Party Applications Overview; Third-Party Application Artifacts; Messaging Applications and Recovering Attachments; Mobile Browsers; Secure Chat Applications

SECTION 2: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they surely will be part of an investigation that comes across your desk. Unfortunately, gaining access to these devices isn't as easy as it used to be. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills to bypass locked Androids and correctly interpret the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics. Android backups can be created for forensic analysis or by a user. Smartphone examiners need to understand the file structures and how to parse these data. Additionally, Android and Google cloud data store tons of valuable information. You will find Google artifacts from iOS users as well.

Topics: Android Acquisition Considerations; Android File System Structures; Handling Locked Android Devices; Android Evidentiary Locations; Traces of User Activity on Android Devices

SECTION 4: iOS Backups, Malware and Spyware Forensics, and Detecting Evidence Destruction

iOS backups are extremely common and are found in the cloud and on hard drives. Users create backups, and we often find that our best data can be derived from creating an iOS backup for forensic investigation. This section will cover methodologies to extract backups and cloud data and analyze the artifacts for each. Malware affects a plethora of smartphone devices. We will examine various types of malware, how it exists on smartphones, and how to identify and analyze it. Most commercial smartphone tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in this class. We'll conduct five labs in this course section alone! The section ends with students challenging themselves using tools and methods learned throughout the course to recover user data from intentionally altered smartphone data (deleting, wiping, and hiding of data).

Topics: iOS Backup File Forensics; Locked iOS Backup Files; iCloud Data Extraction and Analysis; Malware and Spyware Forensics; Detecting Evidence Destruction

SECTION 6: Smartphone Forensics Capstone Exercise

This final course section will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

Topics: Identification and Scoping; Forensic Examination; Forensic Reconstruction

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- Accident reconstruction investigators
- IT auditors
- Graduates of SANS SEC575, SEC563, FOR500, FOR508, FOR572, FOR526, FOR610, or FOR518 who want to take their skills to the next level

Live Online **sans.org/live-online**

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
SANS 2021	Mar 22
DFIRCON Spring	May 3

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**

GREM
Reverse Engineering Malware
giac.org/grem

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Uncover and analyze malicious JavaScript and other components of web pages, which are often used by exploit kits for drive-by attacks
- Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
- Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
- Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files
- Derive Indicators of Compromise (IOCs) from malicious executables to strengthen incident response and threat intelligence efforts

> **"The theory of this course in combination with the labs is a great introduction to the possibilities and approaches one can take when fighting malware."**
>
> — Max de Bruijn, **Fox-IT**

Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen's capabilities by interacting with the malicious program.

The course continues by discussing essential assembly language concepts relevant to reverse engineering. You will learn to examine malicious code with the help of a disassembler and a debugger in order to understand its key components and execution flow. In addition, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by malicious programs.

Next, you will dive into the world of malware that thrives in the web ecosystem, exploring methods for assessing suspicious websites and de-obfuscating malicious JavaScript to understand the nature of the attack. You will also learn how to analyze malicious Microsoft Office, RTF, and PDF files. Such documents act as a common infection vector as a part of mainstream and targeted attacks. You will also learn how to examine "file-less" malware and malicious PowerShell scripts.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files' structure to bypass the packer's protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

The course culminates with a series of Capture-the-Flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical, hands-on malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systemic manner. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

FOR610: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Malware Analysis Fundamentals

Section 1 lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in several phases. Static properties analysis examines meta data and other file attributes to perform triage and determine the next course of action. Behavioral analysis focuses on the program's interactions with its environment, such as the registry, file system, and network. Code analysis focuses on the specimen's inner workings and makes use of debugging tools such as x64bg. You will learn how to set up and use a flexible laboratory to perform such an analysis in a controlled manner, becoming familiar with the supplied Windows and Linux (REMnux) virtual machines. You will then learn how to begin examining malware in your lab with guidance and explanations from the instructor to reinforce the concepts discussed throughout the section.

Topics: Assembling a Toolkit for Effective Malware Analysis; Examining Static Properties of Suspicious Programs; Performing Behavioral Analysis of Malicious Windows Executables; Performing Static and Dynamic Code Analysis of Malicious Windows Executables; Interacting with Malware in a Lab to Derive Additional Behavioral Characteristics

SECTION 2: Reversing Malicious Code

Section 2 focuses on examining malicious Windows executables at the assembly level. You will discover approaches for studying the building blocks of a specimen by looking at it through a disassembler. The section begins with an overview of key code-reversing concepts and presents a primer on essential x86 Intel assembly concepts, such as instructions, function calls, variables and jumps. You will also learn how to examine common assembly constructs such as functions, loops, and conditional statements. The material will then build on this foundation and expand your understanding to make you feel comfortable examining assembly instructions frequently seen in malware. Throughout the discussion, you will learn to recognize common characteristics at a code level, including HTTP command and control, keylogging, and command execution.

Topics: Understanding Core x86 Assembly Concepts to Perform Malicious Code Analysis; Identifying Key Assembly Logic Structures with a Disassembler; Following Program Control Flow to Understand Decision Points During Execution; Recognizing Common Malware Characteristics at the Windows API Level (Registry Manipulation, Keylogging, HTTP Communications, Droppers); Extending Assembly Knowledge to Include x64 Code Analysis

SECTION 3: Malicious Web and Document Files

Section 3 focuses on examining malicious web pages and documents, which adversaries can use to directly perform malicious actions on the infected system and launch attacks that lead to the installation of malicious executable files. The section begins by discussing how to examine suspicious websites that might host client-side exploits. Next, you will learn how to deobfuscate malicious scripts with the help of script debuggers and interpreters, examine malicious Microsoft Office macros, and assess the threats associated with PDF and RTF files using several techniques.

Topics: Interacting with Malicious Websites to Assess the Nature of Their Threats; De-obfuscating Malicious JavaScript Using Debuggers and Interpreters; Analyzing Suspicious PDF Files; Examining Malicious Microsoft Office Documents, Including Files with Macros; Analyzing Malicious RTF Document Files

SECTION 4: In-Depth Malware Analysis

Section 4 builds on the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. The section begins by discussing how to handle packed malware. We will examine ways to identify packers and strip away their protection with the help of a debugger and other utilities. We will also walk through the analysis of malware that employs multiple technologies to conceal its true nature, including the use of registry, obfuscated JavaScript and PowerShell scripts, and shellcode. Finally, we will learn how malware implements spyware and usermode rootkit functionality to perform code injection and API hooking, examining this functionality from both code and memory forensics perspectives.

Topics: Recognizing Packed Malware; Getting Started with Unpacking; Using Debuggers for Dumping Packed Malware from Memory; Analyzing Multi-Technology and Fileless Malware; Code Injection and API Hooking; Using Memory Forensics for Malware Analysis

SECTION 5: Examining Self-Defending Malware

Section 5 takes a close look at the techniques that malware authors commonly use to protect malicious software from being examined. You will learn how to recognize and bypass anti-analysis measures designed to slow you down or misdirect you. In the process, you will gain more experience performing static and dynamic analysis of malware that is able to unpack or inject itself into other processes. You will also expand your understanding of how malware authors safeguard the data that they embed inside malicious executables. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

Topics: How Malware Detects Debuggers and Protects Embedded Data; Unpacking Malicious Software that Employs Process Hollowing; Bypassing the Attempts by Malware to Detect and Evade the Analysis Toolkit; Handling Code Misdirection Techniques, including SEH and TLS Callbacks; Unpacking Malicious Executable by Anticipating the Packer's Actions

SECTION 6: Malware Analysis Tournament

Section 6 assigns you to the role of a malware analyst working as a member of an incident response or forensics team. You will be presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further your ability to perform typical malware analysis tasks and offer additional learning opportunities. The challenges are designed to reinforce skills covered in the first five sections of the course, making use of the popular SANS NetWars educational platform. By applying the techniques learned earlier in the course, you will consolidate your knowledge and shore up skill areas where you might need additional practice.

Topics: Behavioral Malware Analysis; Dynamic Malware Analysis (Using a Debugger); Static Malware Analysis (Using a Disassembler); JavaScript De-obfuscation; PDF Document Analysis; Office Document Analysis; Memory Analysis

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skill sets and learn how to play a pivotal role in the incident response process

Live Online **sans.org/live-online**

EVENT	START DATE
CTI Summit	Jan 25
Scottsdale: Virtual Edition	Feb 22
SANS 2021	Mar 22
Cyber Security Mountain: April	Apr 5
DFIRCON Spring	May 3
Cyber Security Central: June	Jun 7

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

MGT414: **SANS Training Program for CISSP® Certification**

GISP
Information Security Professional
giac.org/gisp

6	46	Laptop
Day Program	CPEs	Not Needed

You Will Be Able To

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

> **"This training was a comprehensive overview of all topics covered in the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless."**
>
> — Ron Pinnock, **Navy Exchange Service Command**

Need training for the CISSP® exam?

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)^2 that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

After completing the course students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)^2.

Course Authors' Statement

"The CISSP® certification has been around for nearly 25 years. The exam is designed to test your understanding of the Common Body of Knowledge, which may be thought of as the universal language of information security professionals. It is often said to be a mile wide and two inches deep. The CISSP® exam covers a lot of theoretical information that is critical for a security professional to understand. However, this material can be dry, and since most students do not see the direct applicability to their jobs, they find it boring. The goal of this course is to bring the eight domains of knowledge of the CISSP® to life. The practical workings of this information can be discovered by explaining important topics with stories, examples, and case studies. We challenge you to attend the SANS CISSP® training course and find the exciting aspect of the eight domains of knowledge!"
—Eric Conrad and Seth Misenar

> **"This class focuses like a laser on the key concepts you will need to understand the CISSP® exam. Do not struggle with thousand page textbooks. Let this course be your guide!"**
>
> — Carl Williams, **Harris Corporation**

MGT414: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Introduction; Security and Risk Management

In the first section of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

SECTION 2: Asset Security and Security Engineering – Part 1

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of Section 2, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

Topics: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

SECTION 3: Security Engineering – Part 2; Communication and Network Security

This course section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

Topics: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

SECTION 4: Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like Oauth and OpenID.

Topics: Domain 5: Identity and Access Management

SECTION 5: Security Assessment and Testing; Security Operations

This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as the cloud, and we'll wrap up section five with a deep dive into disaster recovery.

Topics: Domain 6: Security Assessment; Domain 7: Security Operations

SECTION 6: Software Development Security

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be "baked in" as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

> **"Great discussions and examples that provide a clear understanding and relate material to examples."**
>
> — Kelley ONeil, **Wells Fargo**

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel and contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
Scottsdale: Virtual Edition	Feb 22
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Rocky Mountain Spring	Apr 26
Security West	May 10
Miami: Virtual Edition	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

MGT512: **Security Leadership Essentials for Managers**

GSLC
Security Leadership
giac.org/gslc

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

Course Author Statement

"I have found that technical professionals who are taking on management responsibility need to learn how to convey security concepts in ways that non-technical people can understand. At the same time, managers who are new to security need to learn more about the different domains of cybersecurity. In both cases, there is a need to learn about the work of managing security. That is why this course focuses on the big picture of securing the enterprise, from governance all the way to the technical security topics that serve as the foundation for any security manager. Ultimately, the goal of the course is to ensure that you, the advancing manager, can make informed choices to improve security at your organization."
— Frank Kim

> **"SANS prepared me for the [GSLC] certification and provided valuable information that I can use on the job immediately. Networking with peers and SANS@NIght provided extra value that's not normally available at other training sessions."**
>
> — Rick Derks, **FCS Financial**

Leading Security Initiatives to Manage Information Risk

Security managers need both technical knowledge and management skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics.

This course empowers you to become an effective security manager and get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle, including governance and technical controls focused on protecting, detecting, and responding to security issues.

This course will prepare you to:

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage technical personnel
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Lead a Security Operations Center (SOC)
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud
- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

How the Course Works

MGT512 uses case scenarios, group discussions, team-based exercises, in-class games, and a security leadership simulation to help students absorb both technical and management topics.

The course uses the Cyber42 leadership simulation game. This web-application-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

MGT512: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Building Your Security Program

The course starts with a tour of the information and topics that effective security managers and leaders must know to function in the modern security environment. This includes an understanding of the different types of cybersecurity frameworks available to structure your security team and program. Risk is central to effective information security management, and key risk concepts are discussed to lay the foundation for effective risk assessment and management. Security policy is a key tool that security managers use to manage risk. We'll cover approaches to policy to help you plan and manage your policy process. Finally, security functions, reporting relationships, and roles and responsibilities are discussed to give the advancing manager a view into effective security team and program structure.

Topics: Security Frameworks; Understanding Risk; Security Policy; Program Structure

SECTION 3: Protecting Data and Systems

Section 3 focuses on protecting data and systems. This includes building an understanding of cryptography concepts, encryption algorithms, and applications of cryptography. Since encrypting data alone is not sufficient, we'll discuss the distinction between privacy and security to give managers a primer on key privacy concepts. To implement new initiatives, security leaders must also develop negotiating skills and the ability to manage highly technical team members. Finally, we cover security awareness, which is a huge component of any security program that must drive activities that lead to changes in human behavior and create a more risk-aware and security-aware culture.

Topics: Data Protection; Negotiations Primer; Privacy Primer; Security Awareness

SECTION 5: Detecting and Responding to Attacks

Section 5 focuses on detection and response capabilities. This includes gaining appropriate visibility via logging, monitoring, and strategic thinking about a security information and event management (SIEM) system. When making a large investment, such as a SIEM, managers must also conduct a thorough analysis of vendors. Once implemented, the logs in a SIEM are a core component of any Security Operations Center (SOC). We'll discuss the key functions of a SOC along with how to manage and organize your organization's security operations. The incident response process is discussed in relation to identifying, containing, eradicating, and recovering from security incidents. This leads into a discussion of longer-term business continuity planning and disaster recovery. Managers must also understand physical security controls that, when not implemented appropriately, can cause technical security controls to fail or be bypassed. The course ends with a war game that simulates an actual incident. This tabletop simulation contains a number of injects or points at which students are presented with additional information to which they can respond. After dealing with the incident itself, the simulation concludes with a game focused on choosing appropriate security controls to mitigate future incidents.

Topics: Logging and Monitoring; Vendor Analysis; Security Operations Center; Incident Response; Contingency Planning; Physical Security

SECTION 2: Protecting Networks and Systems

Section 2 provides foundational knowledge to protect networks and systems. This includes a thorough discussion of network security that is modeled around the various layers of the network stack. This leads into a discussion on building a vulnerability management program and the associated process to successfully find and fix vulnerabilities. Finally, we cover malware and attack examples and corresponding host security controls for the endpoint and server. These topics give managers a deeper understanding of what their teams are talking about and where various issues and protections lay within the seven layers of the network model.

Topics: Network Security; Vulnerability Management; Host Security

SECTION 4: Leading Modern Security Initiatives

Section 4 covers what managers need to know about leading modern security initiatives. Managers must be knowledgeable about software development processes, issues, and application vulnerabilities. We'll look at the secure SDLC, OWASP Top Ten, and leading-edge development processes built on DevSecOps. For any project or initiative, security leaders must also be able to drive effective project execution. Having a well-grounded understanding of the project management process makes it easier to move these projects forward. We'll also discuss modern infrastructure-as-code approaches and tools to automate consistent deployment of standard configurations. The cloud is a major initiative that many organizations are either tackling now or planning to undertake. To get ready for these initiatives, we'll provide an overview of Amazon Web Services (AWS) to serve as a reference point and discuss key cloud security issues based on the Cloud Security Alliance guidance. The cloud, the rise of mobile devices, and other factors are highlighting weaknesses in traditional, perimeter-oriented security architectures. This leads to a discussion of the Zero Trust Model.

Topics: Application Security; DevSecOps; Project Management; Infrastructure as Code; Cloud Security; Modern Security Architecture

> **"MGT512 is valuable because it is relevant/current to the security landscape from my management vantage point."**
>
> — Michael Bradley, **Prudential Financial**

Who Should Attend

- Security Managers
  - Newly appointed information security officers
  - Recently promoted security leaders who want to build a security foundation for leading and building teams
- Security Professionals
  - Technically skilled security administrators who have recently been given leadership responsibilities
- Managers
  - Managers who want to understand what technical people are telling them
  - Managers who need an understanding of security from a management perspective

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
Cyber Security East: Feb	Feb 22
Cyber Security West: March	Mar 15
Leadership & Cloud Security	Mar 29
Cyber Security East: April	Apr 12
Baltimore Spring: Virtual Edition	Apr 26
Security West	May 10
Security Leadership: May	May 24
SOC Training	Jun 14
Security Leadership: June	Jun 28

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

MGT514: **Security Strategic Planning, Policy, and Leadership**

GSTRT
Strategic Planning, Policy & Leadership
giac.org/gstrt

5 Day Program	30 CPEs	Laptop Not Needed

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

> **"This course provided a full scope of leadership and security that can immediately be applied to your job."**
>
> — Jerry Butler, **NAVSEA OOI**

Author Statement

"This is the course I wish I had taken when I first started my career. You don't have to wait until you are in a management position to focus on your strategic planning, management, and leadership skills. Have you ever found yourself in a situation where you thought, 'Something I'm doing isn't working'? This course will set you on the path to address that concern. It's commonly stated that to succeed as a modern security leader you need to understand and align with the business to support the organization's mission. But what does that actually mean in practice? Instead of trying to get there on your own, join us to learn practical tools and lessons that have worked for countless other leaders, security officers, and CISOs."

— Frank Kim

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams. The course will help you to:

- **Develop Strategic Plans**
  Strategic planning is hard for IT and security professionals because we spend so much time responding and reacting. We almost never do strategic planning until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. MGT514 will teach you how to develop strategic plans that resonate with other IT and business leaders.
- **Create Effective Information Security Policy**
  Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and responded by saying "No way, I am not going to do that?" Most of us have. Policy must be aligned with an organization's culture. In MGT514, we break down the steps to policy development so that you have the ability to design and assess policies that can successfully guide your organization.
- **Develop Management and Leadership Skills**
  Leadership is a skill that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and having the vision to see and effectively use available resources toward the end goal.

  Effective leadership entails persuading team members to accomplish their objectives, removing the obstacles preventing them from doing it, and maintaining the well-being of the team in support of the organization's mission. MGT514 will teach you to use management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

MGT514 uses the Cyber42 leadership simulation game to put you in situations that spur discussion, critical thinking, and melding of different points of view that you will encounter at work.

The course also uses case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world situations. You will be able to use these same activities with your own team members at work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will understand the different phases of the strategic planning process, learn key planning tools, and have the fundamental skills to create strategic plans that protect your company, enable key innovations, and facilitate working effectively with your business partners.

MGT514: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Foundations of Strategic Planning

Creating security strategic plans requires a fundamental understanding of the business and a deep understanding of the threat landscape. Deciphering the history of the business ensures that the work of the security team is placed in the appropriate context. Stakeholders must be identified and appropriately engaged within this framework. This includes understanding their motivations and goals, which is often informed by the values and culture your organization espouses. Successful security leaders also need a deep understanding of business goals and strategy. This business understanding needs to be coupled with knowledge of the threat landscape – including threat actors, business threats, and attacker tactics, techniques, and procedures – that informs the strategic plan.

Topics: Decipher the Business; Decipher the Threats

SECTION 2: Strategic Roadmap Development

With a firm understanding of the drivers of business and the threats facing the organization, you will develop a plan to analyze the current situation, identify the target state, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today (2) what you should be doing in the future (3) what you don't want to do, and (4) what you should do first. Once this plan is in place, you will learn how to build and execute it by developing a business case, defining metrics for success, and effectively marketing your security program.

Topics: Define the Current State; Develop the Plan; Deliver the Program

SECTION 3: Security Policy Development and Assessment

Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedures. This includes knowing the role of policy in protecting the organization along with its data, systems, and people. In developing policy, you also need to know how to choose the appropriate language and structure so that it fits with your organization's culture. As policy is developed you must manage the entire lifecycle from approval and socialization to measurement in order to make necessary modifications as time goes on. This is why assessing policy and procedure is so important. Policy must keep up to date with the changing business and threat landscape.

Topics: Purpose of Policy; Develop Policy; Managing Policy; Assess Policy and Procedure

SECTION 4: Leadership and Management Competencies

This course section will teach the critical skills you need to lead, motivate, and inspire your teams to achieve your organization's goals. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership, you will understand how to motivate employees and develop from a manager into a leader.

Topics: Why Choose Leadership; Essential Leadership; Build Effective Teams; Engage Teams; Effective Communication; Leading Change

SECTION 5: Strategic Planning Workshop

Using case studies, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. The case studies are taken directly from Harvard Business School, which pioneered the case study method. The case studies focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, enabling students to synthesize and apply concepts, management tools, and methodologies learned in class.

Topics: Creating a Presentation for the CEO; Understanding Business Priorities; Enabling Business Innovation; Effective Communication; Stakeholder Management

> **"This course provides invaluable info with specific guidance on how to perform leadership tasks, and it also provides links to useful info...Outstanding."**
>
> — Jeff Haynes, **NELO**

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

Live Online **sans.org/live-online**

EVENT	START DATE
Security East	Jan 11
Scottsdale: Virtual Edition	Feb 22
Leadership & Cloud Security	Mar 29
Cyber Security East: April	Apr 12
Cyber Security Central: May	May 3
Security West	May 10
Security Leadership: May	May 24
Security Leadership: June	Jun 28

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! MGT516: **Managing Security Vulnerabilities: Enterprise and Cloud**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Create, implement, and mature your vulnerability management program
- Establish secure and defensible enterprise and cloud computing environments
- Build an accurate and useful inventory of IT assets in the enterprise and the cloud
- Identify existing vulnerabilities and understand how to meaningfully use this information
- Better analyze the output of VM tools and related technology to make the data more actionable
- Prioritize vulnerabilities for treatment based on a variety of techniques
- Effectively report and communicate vulnerability data within your organization
- Understand treatment capabilities and better engage with treatment teams
- Make vulnerability management more fun and engaging for all those involved

> **“An understanding of vulnerability management and cloud security is becoming not only valuable but a necessity to keep one’s organization secure in this constantly changing and dynamic environment.”**
>
> — Kae David, EY

Stop Treating Symptoms. Cure The Disease.

This course will show you the most effective ways to mature your vulnerability management program and move from identifying vulnerabilities to successfully treating them. You will learn how to move past the hype to successfully prioritize the vulnerabilities that are not blocked, then clearly and effectively communicate the risk associated with the rest of the vulnerabilities in your backlog that, for a variety of reasons, cannot currently be remediated. You’ll also learn what mature organizations are doing to ease the burden associated with vulnerability management across both infrastructure and applications as well as across both their cloud and non-cloud environments.

MGT516 provides you with the information you need to skillfully fight the VM battle. Learning is reinforced through lab exercises, including the Cyber42 game. The game puts students in the driver’s seat for the fictional Everything Corporation (“E-Corp”). Students will have to select three major initiatives throughout the course that will mature E-Corp’s VM program, and they’ll also need to choose how to respond to 13 realistic events that are sure to have an impact on their program. Depending on how students respond, E-Corp’s security culture and the maturity of the different components of its VM program will be impacted. These tabletop exercises will enable students to put the skills they are learning into practice when they return to work at their own organizations.

Succeed Where Many Are Failing

Vulnerability, patch, and configuration management are not new security topics. In fact, they are some of the oldest security functions. Yet, we still struggle to manage these capabilities effectively. The quantity of outstanding vulnerabilities for most large organizations is overwhelming, and all organizations struggle to keep up with the never-ending onslaught of new vulnerabilities in their infrastructure and applications. When you add in the cloud and the increasing speed with which all organizations must deliver systems, applications, and features to both their internal and external customers, security may seem unachievable.

This course highlights why many organizations are still struggling with vulnerability management and shows students how to solve these challenges. How do we manage assets successfully and analyze and prioritize vulnerabilities? What reports are most effective? How do we deal with vulnerabilities in our applications, and how do we treat them? How do we make vulnerability management fun and get everyone to engage in the process? We’ll not only answer these questions, but also examine how the answers change as we move to the cloud, implement the private cloud, or roll out DevOps within our organizations.

The primary goal of this course is to help you succeed where many are failing and to present solutions to the problems many organizations are experiencing or will experience as they mature. Whether your vulnerability management program is well established or just starting, this course will help you think differently about vulnerability management.

By understanding common issues and how to solve them, you will be better prepared to meet the challenges ahead and guide your IT teams and the broader organization to successfully treat vulnerabilities. Through discussion-based labs and other exercises in the MGT516 course, you will learn specific analysis and reporting techniques. The Cyber42 game will allow you to experience the issues you may face when building out your own program or responding to events in your environment.

Knowing that our environments are adopting cloud services and becoming more tightly integrated with them, we’ll look at both cloud and non-cloud environments simultaneously throughout the course, highlighting the tools, processes, and procedures that can be leveraged in each environment and presenting new and emerging trends.

A capstone exercise during the final course section of MGT516 features a business scenario that includes both enterprise and cloud-based environments. The exercise allows students to analyze and discuss how best to implement and maintain a vulnerability management program and leverage some of the information they have learned throughout the course. The group solutions are then reviewed in class so participants can learn what others outside their group have determined would best help the organization in the scenario succeed.

MGT516: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Overview: Cloud and Asset Management

In this section we look at why vulnerability management is important and introduce the course. We then provide an overview of the cloud and how different cloud service types and architectures can impact the way we manage vulnerabilities. We'll also look at how to choose technologies and tools for our cloud environments. Finally, we'll dig into why asset management is so important and foundational for effective vulnerability management, and the different ways that gaining additional context can help us succeed.

Topics: Course Overview; Cloud and Cloud Vulnerability Management; Asset Management

SECTION 2: Identify

Identifying vulnerabilities continues to be a major focus for our security programs, as it can provide insight into the current risks to our organization. It also provides the data for our analysis and for the measures and metrics we use to guide the program and track our maturity. In this section, we will look at common identification pitfalls and discuss identification architecture and design across both infrastructure and applications. We'll also look at where we might require permission to perform identification and how we safely grant permission to third parties to test our systems and applications and responsibly disclose any findings.

Topics: Identification

SECTION 3: Analyze and Communicate

Gone are the days when we can just scan for vulnerabilities and send the raw output to our teams for remediation. We need to help reduce the burden by analyzing the output to reduce inaccuracies and identify root-cause issues that may be preventing remediation. Once we have identified the issues that cannot be resolved, we should prioritize the rest to ensure that we are having the greatest impact and provide targeted reports or dashboards to system and platform owners. In this section, we will look at some common inaccuracies in the output of our identification processes, discuss prioritization, and then look at what metrics are commonly used to measure our program and the related operational capabilities. We will also discuss how to generate meaningful reports, communication strategies, and the different types of meetings that should be held to increase collaboration and participation.

Topics: Analyze; Communicate

SECTION 4: Treat

Treating vulnerabilities and reducing risk is the ultimate goal of all that we do in vulnerability management. It is important for program managers and all participants to understand the typical processes and technologies that exist and how to leverage them to increase positive change within the organization. Most organizations will have some type of change, patch, and configuration management program. In this course section, we will look at how we interface with these processes to streamline change and increase consistency. We'll also examine some unique challenges we face in the cloud, how to better deal with application vulnerabilities, and some alternatives we can look to when traditional treatment methods are not available.

Topics: Treatment of Vulnerabilities

SECTION 5: Buy-in, Program, and Maturity

Vulnerability management is not the easiest job in an organization, and there are many challenges that can hold us back. From split responsibility and accountability to reliance on shared personnel, much of the work done in this space goes unrecognized. In this section, we'll summarize much of what we have learned and discussed throughout the course and look at how we can use this information to improve the program. We'll discuss how we can make VM more fun and successful within the organization, how we can identify and collaborate more effectively with various stakeholders, and how we can build out and mature a robust vulnerability management program.

Topics: Buy-In, Program; Maturity

> **"Great course, great content. MGT516 is essential for both well-established and developing vulnerability management teams."**
>
> — Robert Adams, **CBC**

The course is based on the Prepare, Identify, Analyze, Communicate, and Treat (**PIACT**) Model:

- **Prepare:** Define, build, and continuously improve the program
- **Identify:** Identify vulnerabilities present in our operating environments
- **Analyze:** Analyze and prioritize identified vulnerabilities and other program metrics to provide meaningful assistance and guidance to stakeholders and program participants
- **Communicate:** Present the findings from analysis appropriately and efficiently for each stakeholder group
- **Treat:** Implement, test, and monitor solutions to vulnerabilities, vulnerability groups, and broader issues identified by the program

Who Should Attend

- CISOs
- Information security managers, officers, and directors
- Information security architects, analysts, and consultants
- Aspiring information security leaders
- Risk management professionals
- Business continuity and disaster recovery planners and staff members
- IT managers and auditors
- IT project managers
- IT/system administration/network administration professionals
- Operations managers
- Cloud service managers and administrators
- Cloud service security and risk managers
- Cloud service integrators, developers, and brokers
- IT security professionals managing vulnerabilities in the enterprise or cloud
- Government IT professional who manage vulnerabilities in the enterprise or cloud (FedRAMP)
- Security or IT professionals who have team-lead or management responsibilities
- Security or IT professionals who use or are planning to use cloud services

Live Online **sans.org/live-online**

EVENT	START DATE
Cloud Defender	Jan 11
Scottsdale: Virtual Edition	Feb 22
Leadership & Cloud Security	Mar 29
Pen Test Austin: Virtual Edition	Apr 19
Security West	May 10
CloudSec Next Summit	Jun 7
Cyber Security Mountain: June	Jun 21

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! MGT521: **Leading Cybersecurity Change: Building a Security-Based Culture**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- More effectively communicate to your Board of Directors and executives, collaborate with your peers, and engage your workforce
- Explain what culture is, its importance to cybersecurity, and how to map and measure both your organization's overall culture and security culture
- Align your cybersecurity culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- Explain what organizational change is, identify different models for creating change, and learn how to apply those models
- Enable and secure your workforce by integrating cybersecurity into all aspects of your organization's culture
- Dramatically improve both the effectiveness and impact of large-scale security initiatives
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives and security in general
- Leverage numerous templates and resources from the Digital Download Package and Community Forum that are part of the course and which you can then build on right away

Cybersecurity management is no longer just about technology. It is ultimately about organizational change - change not only in how people think about security but in what they prioritize and how they act, from the Board of Directors to every corner of the organization. Organizational change is a field of management study that enables leaders to analyze, plan, and then improve their operations and structures by focusing on people and culture.

Drawing on real-world lessons from around the world, the SANS MGT521 course will teach you how to leverage the principles of organizational change in order to develop, maintain, and measure a security-driven culture. Through hands-on instruction and a series of interactive labs and exercises, you will apply the concepts of organizational change to a variety of different security initiatives and quickly learn how to embed security into your organization's culture.

Notice to Students

The course is recommended for more senior and/or more experienced cybersecurity managers, officers, and awareness professionals. If you are new to cybersecurity, we recommend some of SANS's more basic courses, such as SEC301, SEC401, or MGT433.

Lab Information

This five-session course includes 17 interactive labs that walk you through exercises and apply the lessons learned to a variety of typical real-world situations and challenges. Many of the labs are carried out as teams, ensuring that you learn not only from the course materials but from other students and their experiences. Culture is a very human and global challenge, and as such we want to expose you to as many different situations and perspectives as possible. **No Laptop Required. "Labs" are group case studies with no computers needed.**

What You Will Receive

- Digital Download Package: A collection of templates, checklists, matrices, reports, and other resources that will help you in your cybersecurity career. This package is continually updated and is based on resources that real cybersecurity leaders have used in developing their own cybersecurity cultures. Why reinvent the wheel when you can reuse or reshape what has worked for others!
- Community Forum: An opportunity to join the private, invitation-only Community Forum dedicated to the human element. The forum currently has over 1,500 active members!
- One 90-day license to the full SSA library of content.

Course Authors Statement

"For far too long, cybersecurity has been perceived as purely a technical challenge. Organizations and leaders are now realizing that we also have to address the human side of cybersecurity management. From securing your workforce's behavior to engaging and training developers, IT staff, and other departments, security today depends on your ability to engage and partner with others. In other words, your security culture is becoming just as important as your technology. MGT521 will provide the frameworks, roadmaps, and skills you need to successfully embed a comprehensive, organization-wide cybersecurity culture. In addition, the course will provide you the resources to measure and communicate the impact to members of your leadership, ensuring their long-term support."

– Lance Spitzner and Russell Eubanks

MGT521: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Fundamentals of Organizational Change

Section 1 begins by demonstrating how cybersecurity management is ultimately about organizational change. Technology alone will no longer solve security problems. We explain what culture is and how it applies to cybersecurity, how to map your organization's overall culture, and then determine the security culture you want and how to align it with your organization's culture. We will then cover organizational change and different models for changing an organizational culture.

Topics: Human Side of Security; Case Study – Equifax Congressional Report; Defining Culture; Mapping Organizational Culture; Defining and Mapping Security Culture; Identifying Desired Security Culture; Defining and Leveraging Change Management Frameworks; Project Charters

SECTION 2: Motivating Change

Section 2 focuses on motivating people and explaining the "why" in change. Far too often, security fails because it dictates what people must do and how to do it but never explains why. As a result, there is a great deal of resistance to attempts to change workforce behavior and implement security initiatives such as DevSecOps or vulnerability management. In this section, we'll walk you through the key elements of explaining why change is needed, including leveraging marketing models, implementing incentive programs, and targeting both specific and global audiences.

Topics: Safety: Survive vs. Thrive; Start With Why; Know Your Audience; Marketing Change; Motivating Global Change; Incentivizing Change; Motivating Stakeholders

SECTION 3: Enabling and Measuring Change

Communicating with people and engaging and motivating them is only half the battle. We also have to enable people to change. This begins with imparting knowledge – that is, training people and providing them with the skills to be successful. We then simplify what is expected of them by making security as easy as possible. Far too often, the policies, processes, and procedures we create are complex, intimidating, or difficult to follow. Finally, we'll cover how to track, measure, and communicate the impact of your change.

Topics: Cognitive Biases; Building Knowledge; Simplifying Security; Measuring Change

SECTION 4: Making the Business Case

Up to this point we have covered how to communicate with your workforce and engage and motivate various departments. In this section we cover how to do the same thing with your business leadership. A strong cybersecurity culture depends on the support of your executives, but to get their support you have to speak their language. In this section we cover the key elements and frameworks for putting together a high-impact business case, including a dive into financials.

Topics: Building Your Business Case; Financing Your Business Case; Communicating Your Business Case

SECTION 5: Capstone Workshop

In this final course section you will combine and apply everything you have learned through a series of labs. Your mission is to work as teams to make some very tough decisions as you attempt to secure Linden Insurance during a crisis. The decisions you and your team make in each lab will impact your team's Culture Score. Each of the six labs builds on the previous labs, with the decisions you make in each lab impacting not only your score but what decisions you can make in future labs – just like in real life!

> **"I am just so happy with this material focusing on embedding secure values into our global culture – exactly what my company needs help with NOW."**
>
> — Lindsay O'Bannon, **Deloitte Global**

Who Should Attend

- Chief information security officers
- Chief risk officers/Risk management leaders
- Security awareness/Engagement managers
- Senior security managers who lead large-scale security Initiatives
- Information security managers, officers, and directors
- Information security architects and consultants
- Aspiring information security leaders
- Business continuity/Disaster recover leaders
- Privacy/Ethics officers

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
Leadership & Cloud Security	Mar 29
Security Leadership: May	May 24
Security Leadership: June	Jun 28

MGT525: **IT Project Management and Effective Communication**

GCPM
Project Manager
giac.org/gcpm

6 Day Program	36 CPEs	Laptop Not Needed

You Will Be Able To

- Recognize the top failure mechanisms related to IT and InfoSec projects, so that your projects can avoid common pitfalls
- Create a project charter that defines the project sponsor and stakeholder involvement
- Document project requirements and create a requirements traceability matrix to track changes throughout the project life cycle
- Clearly define the scope of a project in terms of cost, schedule and technical deliverables
- Create a work breakdown structure defining work packages, project deliverables and acceptance criteria
- Develop a detailed project schedule, including critical path tasks and milestones
- Develop a detailed project budget, including cost baselines and tracking mechanisms
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
- Document project risks in terms of probability and impact, and assign triggers and risk response responsibilities
- Create project earned value baselines and project schedule and cost forecasts

Managing Security Initiatives and IT Projects

SANS MGT525: IT Project Management and Effective Communication provides the training necessary to maintain the Project Management Professional (PMP)® and other professional credentials.

During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the PMBOK® Guide and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes. A copy of the PMBOK® Guide is provided to all participants. You can reference the PMBOK® Guide and use your course material along with the knowledge you gain in class to prepare for the GIAC Certified Project Manager Exam and earn PDUs/CPEs to maintain the Project Management Professional (PMP)® and other professional credentials.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

PMP®, PMBOK®, and the PMI Registered Education Provider® logo are registered trademarks of the Project Management Institute, Inc.

Course Author Statement

"Managing projects to completion, with an alert eye on quality, cost, and time, is something most of us need to do on an ongoing basis. In this course, we break down project management into its fundamental components and galvanize your understanding of the key concepts with an emphasis on practical application and execution of service-based IT and InfoSec projects. Since project managers spend the vast majority of their time communicating with others, throughout the week we focus on traits and techniques that enable effective technical communication. As people are the most critical asset in the project management process, effective and thorough communication is essential."
— Jeff Frisk

> **"I've been managing multi-million dollar projects for years but always felt muddled as to the formal activities required. After the SANS MGT525 project management course, things have become clear at last."**
>
> — Matt Harvey, **U.S. Department of Justice**

MGT525: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Project Management Structure and Framework

This course section offers insight and specific techniques that both beginner and experienced project managers can utilize. The structure and framework section lays out the basic architecture and organization of project management. We will cover the common project management group processes, the difference between projects and operations, project life cycles, and managing project stakeholders.

Topics: Definition of Terms and Process Concepts; Group Processes; Project Life Cycle; Types of Organizations; PDCA Cycle

SECTION 2: Project Charter and Scope Management

During Section 2, we cover project charter and scope management. We will go over techniques used to develop the project charter and formally initiate a project. The scope portion defines the important input parameters of project management and gives you the tools to ensure that from the onset your project is well defined. We cover tools and techniques that will help you define your project's deliverables and develop milestones to gauge performance and manage change requests.

Topics: Formally Initiating Projects; Project Charters; Project Scope Development; Work Breakdown Structures; Scope Verification and Control

SECTION 3: Schedule and Cost Management

Our third section details the schedule and cost aspects of managing a project. We will cover the importance of correctly defining project activities, project activity sequence, and resource constraints. We will use milestones to set project timelines and task dependencies along with learning methods of resource allocation and scheduling. We introduce the difference between resource and product-related costs and go into detail on estimating, budgeting, and controlling costs. You will learn techniques for estimating project cost and rates as well as budgeting and the process for developing a project cost baseline.

Topics: Process Flow; Task Lead and Lag Dependencies; Resource Breakdown Structures; Task Duration Estimating; Critical Path Scheduling; Cost Estimating Tools; Cost vs. Quality; Cost Baselining; Earned Value Analysis and Forecasting

SECTION 4: Communications and Project Resources

During Section 4, we move into project and human resource management and building effective communications skills. People are the most valuable asset of any project and we cover methods for identifying, acquiring, developing and managing your project team. Performance appraisal tools are offered as well as conflict management techniques. You will learn management methods to help keep people motivated and provide great leadership. The effective communication portion of the section covers identifying and developing key interpersonal skills. We cover organizational communication and the different levels of communication as well as common communication barriers and tools to overcome these barriers.

Topics: Acquiring and Developing Your Project Team; Organizational Dependencies and Charts; Roles and Responsibilities; Team Building; Conflict Management; Interpersonal Communication Skills; Communication Models and Effective Listening

SECTION 5: Quality and Risk Management

Section 5 focuses on quality and risk. You will become familiar with quality planning, quality assurance and quality control methodologies as well as learning the cost of quality concept and its parameters. We define quality metrics and cover tools for establishing and benchmarking quality control programs. We go into quality assurance and auditing as well as using and understanding quality control charts. The risk section goes over known vs. unknown risks and how to identify, assess and categorize risk. We use quantitative risk analysis and modeling techniques so that you can fully understand how specific risks affect your project. You will learn ways to plan for and mitigate risk by reducing your exposure as well as being able to take advantage of risks that could have a positive effect on your project.

Topics: Cost of Quality; Quality Metrics; Continual Process Improvement; Quality Baselines; Quality Control; Change Control; Risk Identification; Risk Assessment; Time and Cost Risks; Risk Probability and Impact Matrices; Risk Modeling and Response

SECTION 6: Procurement, Stakeholder Management, and Project Integration

We close out the course with the procurement aspects of project and stakeholder management, and then integrate all of the concepts presented into a solid, broad-reaching approach. We cover different types of contracts and then the make-versus-buy decision process. We go over ways to initiate strong requests for quotations (RFQ) and develop evaluation criteria, then qualify and select the best partners for your project. Stakeholder communication and management strategies are reinforced. The final session integrates everything we have learned by bringing all the topics together with the common process groups. Using a detailed project management methodology, we learn how to finalize the project management plan and then execute and monitor the progress of your project to ensure success.

Topics: Contract Types; Make vs. Buy Analysis; Vendor Weighting Systems; Contract Negotiations; Stakeholder Communication and Stakeholder Management Strategies; Project Execution; Monitoring Your Project's Progress; Finalizing Deliverables; Forecasting and Integrated Change Control

Who Should Attend

- Individuals interested in preparing for the Project Management Professional (PMP)® Exam
- Security professionals who are interested in understanding the concepts of IT project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk-sensitive projects and applications
- Anyone who would like to utilize effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/design position who works regularly with project management staff

> **"MGT525 offers tools and techniques that will directly improve the planning, execution, and closing of your projects."**
>
> — Michael Long, **ARCYBER**

Live Online sans.org/live-online

EVENT	START DATE
SANS 2021	Mar 22
Security West	May 10

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC566: **Implementing and Auditing the Critical Security Controls – In-Depth**

GCCC
Critical Controls
giac.org/gccc

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Security Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

"SEC566 provides great tools, explanation, and insight!"

— Ryan LeVan, **Trex Company, Inc.**

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches students the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defense."

SANS's in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

The Critical Security Controls are listed on the Sections Description page that follows. The full document describing the Critical Security Controls is posted at the Center for Internet Security.

"SEC566 is truly providing the foundation to elevate my organization's security posture. It has given me the tools to secure our environment and explain why we need to in the first place."

— Keri Powell, **Textron**

SEC566: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Introduction and Overview of the 20 Critical Controls

During Section 1, we will cover an introduction and overview of the Critical Security Controls, laying the foundation for the rest of the class. For each control the following information will be covered, and we will follow the same outline for each control:

- Overview of the Control
- How It Is Compromised
- Defensive Goals
- Quick Win Controls
- Visibility and Attribution Controls
- Configuration and Hygiene Controls
- Advanced Controls
- Overview of Evaluating the Control
- Core Evaluation Test(s)
- Testing/Reporting Metrics
- Steps for Root Cause Analysis of Failures
- Audit/Evaluation Methodologies
- Evaluation Tools
- Exercise to Illustrate Implementation or Steps for Auditing a Control

In addition, Critical Controls 1 and 2 will be covered in depth.

Topics: Critical Control 1: Inventory of Authorized and Unauthorized Devices; Critical Control 2: Inventory of Authorized and Unauthorized Software

SECTION 2: Critical Controls 3, 4, 5, and 6

During Section 2, we will cover Critical Security Controls 3, 4, 5, and 6.

Topics: Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers; Critical Control 4: Continuous Vulnerability Assessment and Remediation; Critical Control 5: Controlled Use of Administrative Privileges; Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

SECTION 3: Critical Controls 7, 8, 9, 10, and 11

During Section 3, we will cover Critical Security Controls 7, 8, 9, 10, and 11.

Topics: Critical Control 7: Email and Web Browser Protections; Critical Control 8: Malware Defenses; Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services; Critical Control 10: Data Recovery Capability (validated manually); Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

SECTION 4: Critical Controls 12, 13, 14, and 15

During Section 4, we will cover Critical Security Controls 12, 13, 14 and 15.

Topics: Critical Control 12: Boundary Defense; Critical Control 13: Data Protection; Critical Control 14: Controlled Access Based on Need to Know; Critical Control 15: Wireless Device Control

SECTION 5: Critical Controls 16, 17, 18, 19, and 20

During Section 5, we will cover Critical Security Controls 16, 17, 18, 19, and 20.

Topics: Critical Control 16: Account Monitoring and Control; Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually); Critical Control 18: Application Software Security; Critical Control 19: Incident Response and Management (validated manually); Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

Course Author Statement

"As I've had the opportunity to talk with information assurance engineers, auditors, and managers over the past 10 years, I've seen frustration in the eyes of these hardworking individuals who are trying to make a difference in their organizations by better defending their data systems. It has even come to the point where some organizations have decided that it's simply too hard to protect their information, and many have started to wonder, is the fight really worth it? Will we ever succeed? We see companies and agencies making headway, but the offense keeps pushing. The goal of this course is to give direction and a realistic hope to organizations attempting to secure their systems.

"This course offers direction and guidance from those in the industry who think through the eyes of the attacker as to what security controls will make the most impact. What better way to play defense than by understanding the mindset of the offense? By implementing our defense methodically and with the mindset of a hacker, we think organizations have a chance to succeed in this fight. We hope this course helps turn the tide."

— James Tarala

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel and contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

> **"Very valuable because it focuses on what matters and provides practical and easy ways to improve security posture."**
>
> — Antonio Sannino, P&G

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security Central: Jan.	Jan 18
Leadership & Cloud Security	Mar 29
Cyber Security Mountain: April	Apr 5
Security Leadership: May	May 24
Security Leadership: June	Jun 28

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

GSNA
Systems and Network Auditor
giac.org/gsna

Course Preview available at: **sans.org/demo**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit web application configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain
- Utilize scripting to build a system that will baseline and automatically audit Linux systems

Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise
- Anyone looking to implement effective continuous monitoring processes within the enterprise

Performing IT security audits at the enterprise level can be a daunting task. How should you determine which systems to audit first? How do you assess the risk to the organization related to information systems and business processes? What settings should you check on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do you turn this into a continuous monitoring process? The material covered in this course will answer all of these questions and more.

AUD507 teaches students how to apply risk-based decision-making to the task of auditing enterprise security.

This track is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, students will have the opportunity to delve into the technical "how-to" for determining the key controls that can be used to provide a high level of assurance to an organization. Real-world examples provide students with tips on how to verify these controls in a repeatable way, as well as many techniques for continuous monitoring and automatic compliance validation. These same real-world examples help the students learn how to be most effective in communicating risk to management and operations staff.

AUD507 allows students to practice new skills in realistic, hands-on labs.

In this course, students learn how to use technical tests to develop the evidence needed to support their findings and recommendations. Each course section affords students opportunities to use the tools and techniques discussed in class, with labs designed to simulate real-world enterprise auditing challenges and to allow the students to use appropriate tools and techniques to solve these problems.

We also go beyond simply discussing the tools students could use; we give them the experience to use the tools and techniques effectively to measure and report on the risk in their organizations. The final section of the course is a lab that lets students challenge themselves by solving realistic audit problems using and refining what they have learned in class.

The skills students learn in AUD507 can be used immediately after class.

Students will leave the course with the know-how to perform effective tests of enterprise security in a variety of areas. The combination of high-quality course content, provided audit checklists, in-depth discussion of common audit challenges and solutions, and ample opportunities to hone their skills in the lab provides a unique setting for students to learn how to be an effective enterprise auditor.

> **"AUD507 provides insight on different aspects related to system configurations and associated risks."**
>
> — Yosra Al-Basha, **Yemen LNG Co.**

Live Online sans.org/live-online

EVENT	START DATE
Cyber Security West: March	Mar 15

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

LEG523: **Law of Data Security and Investigations**

GLEG
Law of Data Security & Investigation
giac.org/gleg

Course Preview available at: **sans.org/demo**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with technology regulations, both in the United States and in other countries
- Evaluate the role and meaning of contracts for technology, including services, software and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate technology law risks before they get out of control
- Implement practical steps to cope with technology law risk
- Better explain to executives what your organization should do to comply with information security and privacy law
- Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence
- Make better use of electronic contracting techniques to get the best terms and conditions
- Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard)

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement personnel
- Privacy officers
- Penetration testers
- Cyber incident and emergency responders from around the world (including the private sector, law enforcement, national guard, civil defense and similar agencies)

LEG523 is constantly updated to address changing trends and current events, including:

- The rising influence of the European Union's General Data Protection Regulation (GDPR) in interpretation of cybersecurty law in the United States and around the world
- Compliance at a time when the operations of some enforcers like courts are delayed or curtailed due to the COVID-19 pandemic
- Facing a cyber crisis? Filing a lawsuit in the courts of another country
- The arrest and criminal indictment of two Coalfire penetration testers in Iowa
- How to balance the right to data privacy versus the right to data security under GDPR and the new California Consumer Privacy Act
- Invoking attorney-client privilege to maintain confidentiality of security assessments such as penetration tests
- Video demonstration of how technical expert witnesses can handle adversarial cross-examination in a live online court hearing
- Form a contract to invite outside incident responders – including police, contractors, National Guard, or civil defense agencies from anywhere in the world – to help with a cyber crisis

New law on privacy, e-discovery, and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the cybersecurity team. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and insurance security questionnaires.

This course covers the law of crime, policy, contracts, liability, compliance, cybersecurity, and active defense – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues, or other investigations.

The Global Information Assurance Certification (GLEG) associated with LEG523 demonstrates to employers that you have absorbed the sophisticated content of this course and are ready to put it to use. This coveted GIAC certification distinguishes any professional – whether a cybersecurity specialist, auditor, lawyer, or forensics expert – from the rest of the pack. It also strengthens the credibility of forensics investigators as witnesses in court and can help a forensics consultant win more business. And the value of the certification will only grow in the years to come as law and security issues become even more interconnected.

The course also provides training and continuing education for many compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, GDPR, and PCI-DSS.

Each successive section of this course builds upon lessons from the earlier sections in order to comprehensively strengthen your ability to help your public or private sector enterprise cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with cybersecurity. We cover topical stories, such as Home Depot's legal and public statements about its payment card breach and lawsuits against QSA security vendor Trustwave filed by cyber insurance companies and credit card issuers (third parties with which Trustwave had no relationship!).

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Professionals from outside the United States attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence, and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

One thing that sets this course apart is its emphasis on ethics. The course teaches practical lessons on ethical performace by cyber defenders and digital investigators.

Live Online sans.org/live-online

EVENT	START DATE
Leadership & Cloud Security	Mar 29
Security West	May 10
Security Leadership: June	Jun 28

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

NEW! SEC488: **Cloud Security Essentials**

GCLD
Cloud Security Essentials
giac.org/gcld

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Identify the risks and risk control ownership based on the deployment models and service delivery models of the various products offered by cloud service providers (CSPs)
- Evaluate the trustworthiness of CSPs based on their security documentation, service features, third-party attestations, and position in the global cloud ecosystem
- Create accounts and use the services of any one the leading CSPs and be comfortable with the self-service nature of the public cloud, including finding documentation, tutorials, pricing, and security features
- Articulate the business and security implications of a multicloud strategy
- Secure access to the consoles used to access the CSP environments
- Use command line interfaces to query assets and identities in the cloud environment
- Use hardening benchmarks, patching, and configuration management to achieve and maintain an engineered state of security for the cloud environment
- Evaluate the logging services of various CSPs and use those logs to provide the necessary accountability for events that occur in the cloud environment
- Configure the command line interface and properly protect the access keys to minimize the risk of compromised credentials
- Use the basic Bash and Python scripts to automate tasks in the cloud
- Implement network security controls that are native to both AWS and Azure
- Employ an architectural pattern to automatically create and provision patched and hardened virtual machine images to multiple AWS accounts
- Use Azure Security Center to audit the configuration in an Azure deployment and identify security issues
- Use Terraform to deploy a complete “infrastructure as code” environment to multiple cloud providers
- Leverage the Cloud Security Alliance Cloud Controls Matrix to select the appropriate security controls for a given cloud network security architecture and assess a CSP’s implementation of those controls using audit reports and the CSP’s shared responsibility model
- Follow the penetration testing guidelines put forth by AWS and Azure to invoke your “inner red teamer” to compromise a full stack cloud application

More businesses than ever are moving sensitive data and shifting mission-critical workloads to the cloud – and not just to one cloud service provider (CSP). Research shows that most enterprises have strategically decided to deploy a multicloud platform, including Amazon Web Services, Azure, Google Cloud, and others.

Organizations are responsible for securing their data and mission-critical applications in the cloud. The benefits in terms of cost and speed of leveraging a multicloud platform to develop and accelerate delivery of business applications and analyze customer data can quickly be reversed if security professionals are not properly trained to secure the organization’s cloud environment and investigate and respond to the inevitable security breaches.

The SANS SEC488: Cloud Security Essentials course will prepare you to advise and speak about a wide range of topics and help your organization successfully navigate both the security challenges and opportunities presented by cloud services. Like foreign languages, cloud environments have similarities and differences, and SEC488 covers all of the major CSPs and thus all of the languages of cloud services.

We will begin by diving headfirst into one of the most crucial aspects of cloud – Identity and Access Management (IAM). From there, we’ll move on to securing the cloud through discussion and practical, hands-on exercises related to several key topics to defend various cloud workloads operating in the different CSP models of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

New technologies introduce new risks. This course will equip you to implement appropriate security controls in the cloud, often using automation to “inspect what you expect.” Mature CSPs have created a variety of security services that can help customers use their products in a more secure manner, but nothing is a magic bullet. This course covers real-world lessons using security services created by the CSPs as well as open-source tools. As mentioned, each course book features hands-on lab exercises to help students hammer home the lessons learned. We progressively layer multiple security controls in order to end the course with a functional security architecture implemented in the cloud.

SEC488: Cloud Security Essentials will prepare you to:

- Navigate your organization through the security challenges and opportunities presented by cloud services
- Identify the risks of the various services offered by cloud service providers (CSPs)
- Select the appropriate security controls for a given cloud network security architecture
- Evaluate CSPs based on their documentation, security controls, and audit reports
- Confidently use the services of any of the leading CSPs
- Articulate the business and security implications of multiple cloud providers
- Secure, harden, and audit CSP environments
- Protect the access keys and secrets used in cloud environments
- Use application security tools and threat modeling to assess the security of cloud-based applications
- Automatically create and provision patched and hardened virtual machine images
- Deploy a complete “infrastructure as code” environment to multiple cloud providers
- Leverage cloud logging capabilities to establish accountability for events that occur in the cloud environment
- Detect and respond to security incidents in the cloud and take appropriate steps as a first responder
- Perform a preliminary forensic file system analysis of compromised cloud resources

RETURN TO TABLE OF CONTENTS

SEC488: Section Descriptions

SECTION 1: Identify and Access Management

The first course section will set the stage for how day-to-day operations could change as an enterprise looks at cloud technologies. Different service and delivery models will influence how a business changes based on the model that is being leveraged. In addition to learning about important cloud fundamentals, students will be able to:

- Identify security holes in their cloud account's IAM service
- Understand what it takes to implement cloud accounts that follow the concept of least privilege access
- Discover and protect various secrets related to cloud service authentication
- Use cloud-vendor-provided IAM analysis tools to automate the discovery of any security shortcomings

Topics: Course Overview; Cloud Accounts; Policies and Permissions; Groups and Roles; Temporary Credentials; Secrets Management; Customer Account Management and External Access; More IAM Best Practices

SECTION 2: Compute and Configuration Management

Section 2 will cover ways to protect the compute elements in cloud providers' Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings. Students will determine early on that there is much more complexity when launching instances or virtual machines in the cloud as opposed to on-premise. As the section progresses, students will learn to:

- Securely deploy a compute instance/virtual machine in CSP environments
- Maintain the running instance throughout its lifecycle
- Create hardened images for re-use in the organization
- Understand the various threats that could affect cloud-based applications
- Lock down cloud storage to prevent spillage of sensitive information

Topics: Secure Instance/Virtual Machine Deployment; Host Configuration Management; Image Management; Application Security; Threat Modeling; Platform as a Service (PaaS) and Software as a Service (SaaS) Challenges; Container Services; Cloud Storage

SECTION 3: Data Protection and Automation

This section will first focus on the protection of data in cloud environments. All too often, we are reading news articles about breaches that come down to a misconfiguration of a cloud service. Students will learn just what to look out for regarding these misconfigurations as well as how to:

- Properly identify and classify their organization's data in various cloud services
- Encrypt data where it resides and as it traverses networks
- Ensure the data is available when it is required
- Leverage Infrastructure as Code (IaC) not only to automate operations, but also to automate security configurations
- Identify gaps in cloud-based productivity services
- Understand how CASBs operate and what benefit they may add to the organization

Topics: Data Classification; Data at Rest Encryption; Availability; Data in Transit Encryption; Lifecycle Management; Infrastructure as Code; Productivity Services; Cloud Access Security Brokers (CASB)

SECTION 4: Networking and Logging

Section 4 is where many network security analysts, engineers, and architects will begin salivating, as they will do a deep dive into the ins and outs of cloud networking and log generation, collection, and analysis to set themselves up for success to defend their IaaS workloads. Students will learn how to:

- Control cloud data flows via network controls
- Add segmentation between compute resources of varying sensitivity levels
- Generate the proper logs, collect those logs, and process them as a security analyst
- Increase the effectiveness of their security solutions by gaining more network visibility
- Detect treats in real time as they occur in the cloud

Topics: Private Cloud Networking; Public Cloud Networking; Network Segmentation; Network Protection Services; Cloud Logging Services; Log Collection and Analysis; Network Visibility; Cloud Detection Services

SECTION 5: Compliance, Incident Response, and Penetration Testing

In Section 5, we'll dive headfirst into compliance frameworks, audit reports, privacy, and eDiscovery to equip you with the information and references to ensure that the right questions are being asked during CSP risk assessments. After covering special-use cases for more restricted requirements that may necessitate the AWS GovCloud or Azure's Trusted Computing, we'll delve into penetration testing in the cloud and finish the section with incident response and forensics. Student will learn to:

- Leverage the Cloud Security Alliance Cloud Controls Matrix to select the appropriate security controls for a given cloud network security architecture and assess a CSP's implementation of those controls using audit reports and the CSP's shared responsibility model
- Use logs from cloud services and virtual machines hosted in the cloud to detect a security incident and take appropriate steps as a first responder according to a recommended incident response methodology
- Perform a preliminary forensic file system analysis of a compromised virtual machine to identify indicators of compromise and create a file system timeline

Topics: Security Assurance; Cloud Auditing; Privacy; Government Clouds; Risk Management; Penetration Testing; Legal and Contractual Requirements; Incident Response and Forensics

SECTION 6: CloudWars

This final section consists of an all-day CloudWars competition to reinforce the topics covered in Sections 1–5. Through this friendly competition, students will answer several challenges made up of multiple choice, fill-in-the-blank, as well as hands-on and validated exercises performed in two CSP environments. They will be given a brand-new environment to deploy in two different cloud vendors and will be tasked to take this very broken environment and make the appropriate changes to increase its overall security posture.

> **"Labs were solid and definitely brought home the objectives. I learned of many features we can implement to make our cloud environments more secure."**
>
> — Bob Hewitt, **Stellar Technology Solutions**

Who Should Attend

Anyone who works in a cloud environment, is interested in cloud security, or needs to understand the risks of using cloud service providers should take this course, including:

- Security engineers
- Security analysts
- System administrators
- Risk managers
- Security managers
- Security auditors
- Anyone new to the cloud!

Live Online sans.org/live-online

EVENT	START DATE
Cloud Defender	Jan 11
Cyber Security West: Feb	Feb 1
Cyber Security East: Feb	Feb 22
SANS 2021	Mar 22
Cyber Security East: April	Apr 12
Rocky Mountain Spring	Apr 26
Security West	May 10
Cyber Security East: May	May 17
CloudSec Next Summit	Jun 7
Cyber Security Mountain: June	Jun 21

NEW! SEC510: **Public Cloud Security: AWS, Azure, and GCP**

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Understand the inner workings of cloud services and Platform as a Service (PaaS) offerings in order to make more informed decisions in the cloud
- Understand the design philosophies that undergird each provider and how these have influenced their services in order to properly prescribe security solutions for them
- Discover the unfortunate truth that many cloud services are adopted before their security controls are fully fleshed out
- Understand Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) in depth
- Understand the intricacies of Identity and Access Management, one of the most fundamental concepts in the cloud and yet one of the least understood
- Understand cloud networking and how locking it down is a critical aspect of defense-in-depth in the cloud
- Analyze how each provider handles encryption at rest and in transit in order to prevent sensitive data loss
- Explore the service offering landscape to discover what is driving the adoption of multiple cloud platforms and to assess the security of services at the bleeding edge
- Understand the complex connections between cloud accounts, providers, and on-premise systems and the cloud
- Perform secure data migration to and from the cloud
- Understand Terraform Infrastructure-as-Code well enough to share it with your engineering team as a starting point for implementing the controls discussed in the course

NOTICE: SEC510: Public Cloud Security: AWS, Azure, and GCP was formerly known as SEC510: Multicloud Security Assessment and Defense. It is the exact same material but with two additional sections of content! The new title better reflects the course content.

Multiple Clouds Require Multiple Solutions

SEC510: Public Cloud Security: AWS, Azure, and GCP teaches you how the major cloud providers work and how to securely configure and use their services and Platform as a Service (PaaS) offerings.

Organizations in every sector are increasingly adopting cloud offerings to build their online presence. However, although cloud providers are responsible for the security of the cloud, their customers are responsible for what they do in the cloud. Unfortunately, the providers have made the customer's job difficult by offering many services that are insecure by default. Worse yet, with each provider offering hundreds of different services and with many organizations opting to use multiple providers, security teams need a deep understanding of the underlying details of the different services in order to lock them down. As the landscape rapidly evolves and development teams eagerly adopt the next big thing, security is constantly playing catch-up in order to avert disaster.

SEC510 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services.

The Big 3 cloud providers alone provide more services than any one company can consume. As security professionals, it can be tempting to limit what the developers use to the tried-and-true solutions of yesteryear. Unfortunately, this approach will inevitably fail as the product development organization sidelines a security entity that is unwilling to change. Functionality drives adoption, not security, and if a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. SEC510 gives you the ability to provide relevant and modern guidance and guardrails to these teams to enable them to move both quickly and safely.

> **"The course went immediately into real-world, useful vulnerabilities and how to remediate them. The teachers are clear in presenting materials and expanding on the concepts an appropriate amount. They take real-time questions and incorporate them into the discussion appropriately."**
>
> — Tom Siu, **Case Western Reserve University**

SEC510: **Section Descriptions**

SECTION 1: Cloud Credential Management

SEC510 starts with a brief overview of the Big 3 cloud providers. We will examine the factors driving adoption of multiple cloud providers and the rise in popularity of Azure and GCP, which historically have lagged far behind AWS. Students will then initialize their lab environment and deploy a modern web application to each of the Big 3 providers. This leads into an analysis of the intricacies of Identity and Access Management (IAM), one of the most fundamental and misunderstood concepts in cloud security. Playing the role of an attacker in their lab environment, students will compromise real IAM credentials using application vulnerabilities and then use them to access sensitive data. The remainder of this section will focus on how to leverage well-written IAM policies to minimize the damage caused by such attacks. Although the ultimate solution is to fix the bug in the application, these strategies can prevent a minor incident from becoming front-page news.

Topics: The Multicloud Movement; Multicloud Security Assessment; Identity and Access Management; Cloud Credential Management; Application Vulnerability Overviews

SECTION 3: Encryption, Storage, and Logging

The first half of Section 3 covers all topics related to encryption in the cloud. Students will learn about each provider's cryptographic key solution and how it can be used to encrypt data at rest. Students will also learn how end-to-end, in-transit encryption is performed in the cloud, such as the encryption between clients, load balancers, applications, and database servers. Proper encryption is not only critical for security; it is also an important legal and compliance consideration. This section will ensure that your organization has all of the information at its disposal to send the auditors packing. The second half of Section 3 covers storing data in the cloud, defense-in-depth mechanisms, access logging, filesystem persistence, and more.

Topics: Cloud Key Management; Encryption with Cloud Services; Cloud Storage Platforms

SECTION 5: Cross-Account and Cross-Cloud Assessment

The course concludes with practical guidance on how to operate an organization across multiple cloud accounts and providers. Many of the topics discussed in the earlier course sections are significantly complicated when moving from a single account to multiple accounts, as well as when the providers are integrated with each other. We will cover these complications, look at automatic security benchmarking utilities, and safely tear down the lab environment.

Topics: Cross-Account Management; Cross-Cloud Integrations; Automated Benchmarking; Summary; Additional Resources

SECTION 2: Cloud Virtual Networks

Section 2 covers how to lock down infrastructure within a virtual private network. As the public cloud IP address blocks are well known and default network security is often lax, millions of sensitive assets are unnecessarily accessible to the public Internet. This section will ensure that none of these assets belong to your organization. The section begins by demonstrating how ingress and egress traffic can be restricted within each provider. Students will analyze the damage that can be done without these controls by accessing a public-facing database and creating a reverse shell session in each environment. We will then eliminate both attack vectors with secure cloud configuration. In addition to introducing additional network defense-in-depth mechanisms, we will discuss cloud-based intrusion detection capabilities to address the network-based attacks we cannot eliminate. Students will analyze cloud traffic and search for indicators of compromise.

Topics: Cloud Virtual Networks; Network Traffic Analysis; Private Endpoints; Advanced Remote Access; Command and Control Servers

SECTION 4: Serverless Platforms

This course section tackles the ever-changing trends in technology by providing in-depth coverage of a paradigm taking the industry by storm: Serverless. It balances the discussion of the challenges serverless introduces with the advantages it provides to secure product development and security operations. The first half of the section covers serverless cloud functions in AWS Lambda, Microsoft Azure, and Google Cloud Functions. After introspecting the serverless runtime environments using Serverless Prey (a popular open-source tool written by the course authors), students will examine and harden practical serverless functions in a real environment. The second half of the course section covers App Services, which often interplay with cloud functions. The section concludes with a detailed analysis of Firebase, an application platform with serverless offerings that has been loosely integrated with the Google Cloud Platform since its acquisition by Google in 2014.

Topics: Cloud Serverless Functions; Application Platforms

Who Should Attend

Security analysts, security engineers, security researchers, cloud engineers, DevOps engineers, security auditors, system administrators, operations personnel, and anyone who is responsible for:

- Evaluating and adopting new cloud offerings
- Researching new vulnerabilities and developments in cloud security
- Identity and Access Management
- Managing a cloud-based virtual network
- Secure configuration management

> **"This course highlighted the three main cloud platforms with their advantages and disadvantages. It taught us how to create users, hack in the systems with vulnerabilities, and then how to harden them."**
>
> — Almami Kassama, **Ahold**

Live Online sans.org/live-online

EVENT	START DATE
Scottsdale: Virtual Edition	Feb 22
Leadership & Cloud Security	Mar 29
Baltimore Spring: Virtual Edition	Apr 26
Security West	May 10
CloudSec Next Summit	Jun 7

SEC522: **Defending Web Applications Security Essentials**

GWEB
Web Application Defender
giac.org/gweb

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Understand the major risks and common vulnerabilities related to web applications through real-world examples
- Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- Fulfill the training requirement as stated in PCI DSS 6.5
- Deploy and consume web services (SOAP and REST) in a more secure fashion
- Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- Strategically roll out a web application security program in a large environment
- Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
- Develop strategies to assess the security posture of multiple web applications

> **"I think SEC522 is absolutely necessary to all techies who work on web applications. I don't think developers understand the great necessity of web security and why it is so important."**
>
> — Mahesh Kandru, **Cabela's**

This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is increasing, and defenders need to learn how to secure these critical data. Traditional network defenses such as firewalls fail to secure web applications. In covering the OWASP Top 10 Risks and beyond, SEC522 will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

The course will present mitigation strategies from an infrastructure, architecture, and coding perspective alongside real-world techniques that have been proven to work. We'll introduce the nature of each vulnerability to help you understand why it happens, then we'll show you how to identify the vulnerability and provide options to mitigate it.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. The focus will be maintained on security strategies rather than coding-level implementation.

SEC522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. You will find the course useful if you are supporting or creating either traditional web applications or more modern web services for a wide range of front ends like mobile applications. The course is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in enhancing the defense of web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- The OWASP Top 10
- Selected specific web application issues from the Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors
- Infrastructure security and configuration management
- Securely integrating cloud components into a web application
- Authentication and authorization mechanisms, including single sign-on patterns
- Application language configuration
- Application coding errors like SQL injection, cross-site request forgery, and cross-site scripting
- Web 2.0 and its use of web services (REST/SOAP)
- Cross-domain web request security
- Business logic flaws
- Protective HTTP headers

The course makes heavy use of hands-on exercises and will conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

SEC522: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Web Fundamentals and Security Configurations

You cannot win the battle if you do not understand what you are trying to defend. The first course section starts with an overview of recent web application attack and security trends, followed by an examination of the essential technologies that are at play in web applications. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

Topics: Introduction to HTTP Protocol; Overview of Web Authentication Technologies; Web Application Architecture; Recent Attack Trends; Web Infrastructure Security/Web Application Firewalls; Managing Configurations for Web Apps

SECTION 2: Defense Against Input-related Threats

Section 2 is devoted to protecting against threats arising from external input. Modern applications have to accept input from multiple sources, such as other applications, browsers, and web services. Web application attacks during the past few years have reminded us that these attack patterns are employed frequently.

Topics: Input-related Vulnerabilities in Web Applications; SQL Injection; Cross-site Request Forgery; Cross-site Scripting Vulnerability and Defenses; Unicode Handling Strategy; File Upload Handling; Business Logic and Concurrency

SECTION 3: Web Application Authentication and Authorization

Section 3 starts with a discussion of authentication in web applications, followed by examples of exploitation and the mitigations that can be implemented in the short and long terms. Considering the trend to move towards less reliance on passwords for authentication, we cover the modern patterns of password-less authentication and multifactor authentications. We complete the discussion by providing information on how to discover and test for vulnerabilities.

Topics: Authentication Vulnerabilities and Defense; Multifactor Authentication; Session Vulnerabilities and Testing; Authorization Vulnerabilities and Defense; SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application

SECTION 4: Web Services and Front-End Security

We'll start Section 4 by focusing on proactive defense mechanisms so that we can be ahead of the bad guys in the game of hack-and-defend. We will cover such topics as handling file uploads, intrusion detection, and the use of deception. The material is designed to give you the extra edge in defending your application.

Topics: Honeytoken; Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; REST Security; Browser-based Defense such as Content Security Policy

SECTION 5: Cutting-Edge Web Security

Section 5 focuses on cutting-edge web application technologies and current research in this area. Topics such as serialization security, clickjacking, and DNS rebinding are covered. These vulnerabilities have emerged and changed in recent years, and we are refining our defense strategies against them. We cover recent developments on these topics and the latest defensive tactics to protect against these attacks.

Topics: Serialization Security; Clickjacking; DNS Rebinding; HTML5 Security; Logging Collection and Analysis for Web Apps; Security Testing; IPv6 Impact on Web Security

> **"As the world moves everything online, SEC522 is a necessity."**
>
> — Chris Spinder, **B/E Aerospace, Inc.**

SECTION 6: Capture-and-Defend-the-Flag Exercise

Section 6 starts by introducing the secure software development life cycle and how to apply it to web development. The main activity will be a large lab that will tie together the lessons learned during the week and reinforce them with hands-on applications. Students will be provided with a virtual machine to implement a complete database-driven dynamic website. In addition, they will use a custom tool to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. Students will then have to decide which vulnerabilities are real and which are false positives, then mitigate the vulnerabilities. The scanner will score the student as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. Students will learn through these hands-on exercises how to secure the web application, starting with securing the operating system and the web server, finding configuration problems in the application language setup, and finding and fixing coding problems on the site.

Topics: Mitigating Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Testing Web Services and Mitigating Security Problems; Reinforcing Key Topics Discussed Throughout the Course through Comprehensive Exercises

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with those requirements

> **"Not only does SEC522 teach the defenses for securing web apps, it also shows how common and easy the attacks are and thus the need to secure the apps."**
>
> — Brandon Hardin, **ITC**

Live Online sans.org/live-online

EVENT	START DATE
Cloud Defender	Jan 11
Cyber Security West: March	Mar 15
Rocky Mountain Spring	Apr 26
CloudSec Next Summit	Jun 7

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC540: **Cloud Security and DevOps Automation**

GCSA
Cloud Security Automation
giac.org/gcsa

5 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Build a Secure DevOps workflow in your organization
- Create automated security tasks in Continuous Integration/Continuous Delivery (CI/CD) systems
- Configure and run scanners from the Secure DevOps toolchain
- Perform cloud infrastructure security audits for common misconfiguration vulnerabilities
- Wire cloud application security scans in cloud-hosted (CI/CD) systems
- Review and identify cloud encryption services for data storage vulnerabilities
- Perform secure secrets management using on-premise and cloud-hosted secrets management tools
- Audit microservice architectures for security vulnerabilities in containers, serverless, and API gateway appliances
- Leverage cloud automation to automate patching and software deployments without downtime
- Build serverless functions to monitor, detect, and actively defend cloud services and configurations

> **"This course definitely makes security in DevOps more relatable and concrete. I love that we are asked to fix issues."**
>
> — Stephen Germain, **Disney**

The cloud moves fast. Automate to keep up.

SEC540 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how DevOps principles, practices, and tools can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

SEC540 examines the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular tools such as Jenkins, GitLab, Puppet, Vault, and Grafana to automate Configuration Management ("Infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), cloud infrastructure, containerization, micro-segmentation, Functions as a Service (FaaS), Compliance as Code, and Continuous Monitoring.

The lab environment starts with an on-premise CI/CD pipeline that automatically builds, tests, and deploys infrastructure and containerized applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques. After laying the DevSecOps foundation, students put their DevSecOps skills to work by deploying and managing a real-world cloud infrastructure. Hands-on exercises deploy containerized workloads in the cloud, integrate on-premise configuration management with Puppet, and manage secrets with HashiCorp Vault and Cloud Key Management Service (KMS). Students analyze and fix cloud infrastructure vulnerabilities, perform cloud-hosted application vulnerability scanning, and defend microservices using tools such as API Gateway and FaaS. Cloud security compliance tools help monitor the infrastructure using code-driven Web Application Firewall (WAF) services, continuous auditing with CloudMapper, and continuous monitoring with Cloud Custodian.

Course Authors' Statement

"DevOps and the cloud are radically changing the way that organizations design, build, deploy, and operate online systems. Leaders like Amazon, Etsy, and Netflix are able to deploy hundreds or even thousands of changes every day, continuously learning, improving, and growing—and leaving their competitors far behind. Now DevOps and the cloud are making their way from Internet 'Unicorns' and cloud providers into enterprises.

"Traditional approaches to security can't come close to keeping up with this rate of accelerated change. Engineering and operations teams that have broken down the 'walls of confusion' in their organizations are increasingly leveraging new kinds of automation, including Infrastructure as Code, Continuous Delivery and Continuous Deployment, microservices, containers, and cloud service platforms. The question is: can security take advantage of the tools and automation to better secure its systems?

"Security must be reinvented in a DevOps and cloud world."

— Ben Allen, Jim Bird, Eric Johnson, and Frank Kim

> **"Great course! Excellent instructor! Lots of hands-on! It definitely met my expectations and I will absolutely recommend it to other people."**
>
> — Sandro Blatter, **SBB**

SEC540: Section Descriptions

Course Preview available at: **sans.org/demo**

SECTION 1: Introduction to DevSecOps

SEC540 starts by introducing DevOps practices, principles, and tools. We will examine how DevOps works, how to work in DevOps, and the importance of culture, collaboration, and automation. We'll use case studies of DevOps "Unicorns" – the Internet tech leaders that have created the DevOps DNA – to consider how and why these leaders succeeded and to examine the keys to their DevOps security programs. We'll then look at Continuous Delivery, which is the DevOps automation engine. We'll explore how to build up a Continuous Delivery or Continuous Deployment pipeline, including how to fold or wire the DevSecOps security controls into the Continuous Delivery pipeline, and how to automate security checks and tests in Continuous Delivery.

Topics: Introduction to the Cloud and DevOps; Case Studies on DevOps Unicorns; Security Challenges in DevOps; DevOps Deployment Kata; Secure Continuous Delivery; Security in Pre-Commit; Security in Commit; Security in Acceptance

SECTION 3: Cloud Security Operations

Students start this section reviewing container orchestration options and scanning and testing their cloud infrastructure code for common cloud misconfiguration vulnerabilities. Correcting and committing infrastructure code changes will trigger an automated infrastructure pipeline to harden the cloud infrastructure code. Next, we will explore cloud continuous integration and delivery tools and leverage serverless computing to perform static analysis and software supply chain vulnerability scans before releasing containers into the orchestration services. We then shift focus to production and operations by building continuous security monitoring using Grafana, CloudWatch, and Slack. Section 3 wraps up with cloud data protection, exploring the various encryption services, how to implement secrets management in the cloud, and how to integrate on-premise secrets with cloud resources.

Topics: Securing Cloud Architecture; Security Scanning in CI/CD; Continuous Security Monitoring; Data Protection and Secrets Management

SECTION 5: Compliance as Code

Expanding on the foundation from previous sections, DevSecOps practitioners now shift to leveraging cloud services to automate security compliance. We start by deploying and configuring a cloud web application firewall with monitoring, attack detection, and active defense capabilities to catch and block bad actors. Next, we implement continuous compliance scanning for cloud misconfigurations. Finally, we work on enforcing policy as code to detect and correct cloud configuration drift.

Topics: Runtime Security Automation; Continuous Auditing; Cloud Security Monitoring

SECTION 2: Cloud Infrastructure and Orchestration

Building on the ideas and frameworks developed in Section 1, we'll examine how Cloud Infrastructure as Code can quickly and consistently deploy new infrastructure and services. Using modern automated configuration management tools like Puppet, Chef, and Ansible, we'll also cover how to enforce desired state configuration for cloud-hosted virtual machines. Since workloads are moving into container services, we'll explore the container security issues associated with tools such as Docker and Kubernetes.

Topics: Cloud Security Fundamentals; Secure Infrastructure as Code; Configuration Management as Code; Container Security Hardening

SECTION 4: Cloud Security as a Service

In this section we'll leverage cloud security services to lock down functional and high-availability systems. Students start by deploying a security patch to an application using blue/green environments to minimize downtime. Shifting focus, we move on to protecting static website content served by a Content Delivery Network (CDN) using private key signing. The second half of this Section 4 explores the world of microservices, protecting APIs with an API Gateway, and deploying serverless functions to manage authorization, data entitlements, and access control.

Topics: Blue/Green Deployment Options; Secure Content Delivery; Microservice Security; Serverless Security

> **"SEC540 opened my eyes to a new way of thinking about operations and security unlike anything since SEC401: Security Essentials Bootcamp Style."**
>
> — Todd Anderson, **OBE**

Who Should Attend

- Anyone working in or transitioning to a public cloud environment
- Anyone working in or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to cloud and DevOps Continuous Delivery pipelines
- Anyone interested in learning how to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS) and Microsoft Azure
- Anyone interested in leveraging cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

Live Online sans.org/live-online

EVENT	START DATE
Cloud Defender	Jan 11
Cyber Security West: Feb	Feb 1
Scottsdale: Virtual Edition	Feb 22
Leadership & Cloud Security	Mar 29
Cyber Security East: April	Apr 12
Baltimore Spring: Virtual Edition	Apr 26
Security West	May 10
CloudSec Next Summit	Jun 7
Cyber Security Mountain: June	Jun 21

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

SEC545: **Cloud Security Architecture and Operations**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Revise and build internal policies to ensure cloud security is properly addressed
- Understand all major facets of cloud risk, including threats, vulnerabilities, and impact
- Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models
- Evaluate Cloud Access Security Brokers to better protect and monitor SaaS deployments
- Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls
- Evaluate basic virtualization hypervisor security controls
- Design and implement network security access controls and monitoring capabilities in a public cloud environment
- Design a hybrid cloud network architecture that includes IPSec tunnels
- Integrate cloud identity and access management into security architecture
- Evaluate and implement various cloud encryption types and formats
- Develop multi-tier cloud architectures in a virtual private cloud, using subnets, availability zones, gateways, and NAT
- Integrate security into DevOps teams, effectively creating a DevSecOps team structure
- Build automated deployment workflows using Amazon Web Services and native tools

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- DevOps and DevSecOps engineers
- System administrators
- Cloud administrators

As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But will information security prove to be an Achilles' heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We'll start with a brief introduction to cloud security fundamentals, then cover the critical concepts of cloud policy and governance for security professionals. For the rest of section one and all of section two, we'll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We'll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We'll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We'll devote an entire section to adapting our offense and defense focal areas to the cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we'll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration and every facet of the cloud life cycle. We'll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.

Hands-on Training

SEC545: Cloud Security Architecture and Operations reinforces knowledge transfer through the use of numerous hands-on labs. This approach goes well beyond traditional lectures and delves into literal application of techniques. Hands-on labs are held during every section to reinforce the skills covered in class and to provide students with experience using tools to implement effective security. The labs are designed to enable students to apply what they are learning in an instructor-led environment. Labs are wide-ranging and include:

- Security-as-a-Service labs
- Architecture and design labs
- Security automation labs
- Offensive and defensive labs in the cloud
- Log collection and review labs
- Playing flAWS, a challenging cloud Capture-the-Flag challenge

> **"SEC545 helped to better align our policies to include cloud systems, and it gave me more insight into cloud systems and their configurations."**
>
> — Craig Lunde, **Discovery Benefits Inc.**

SEC545: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Cloud Service Models and Controls

The course starts with an introduction to the cloud, including terminology, taxonomy, and basic technical premises. We also examine guidance available from the Cloud Security Alliance, including the Cloud Controls Matrix, the 14 major themes of cloud security, and other research available. For most of this section, we will examine the main technical considerations for Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS). We'll start by breaking down SaaS and some of the main types of security controls available, with examples of well-known SaaS provider options. A specialized type of Security-as-a-Service (SecaaS) known as Cloud Access Security Brokers will also be explained, with examples of what to look for in such a service. We'll touch on additional brokering services like Secure Access Service Edge and architecture and control concepts for this. We'll then shift to Platform-as-a-Service (PaaS) controls and architecture, with an emphasis on containers, orchestration, and serverless. We'll break down security controls for all of these in the major cloud providers and outline some suggested security architecture principles and practices to better secure and monitor these environments. Finally, we'll discuss Infrastructure-as-a-Service (IaaS) security, which will set the stage for the rest of the course. Section 1 wraps up with an introduction to virtualization security, which all IaaS environments significantly rely upon.

Topics: Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; SaaS Security Controls and Examples; Cloud Access Security Brokers; Secure Access Service Edge; Intro to PaaS Security Controls; Container Security Controls and Architecture; Orchestration Tools and Security Controls; Serverless Security Controls and Architecture; Introduction to IaaS Security Controls; Virtualization Security

SECTION 2: Cloud Security Architecture and Operations: Part 1

In section 2, we begin our journey into the realm of cloud security architecture and operational design. We'll start by breaking down a number of core architecture principles that can help all organizations use best practices in any project or cloud deployment scenario. Then we'll analyze suggested architecture best practices from the three leading cloud providers. Amazon, Microsoft, and Google all have recommendations that we can dissect and apply to any security design for the cloud. After we cover core security architecture, we'll focus on two of the biggest topic areas: network security and identity and access management (IAM). We'll start by breaking down cloud-native network security controls in all of the major providers, then comparing traditional on-premise network controls to the cloud. Then we'll look at network security architecture models, comparing and contrasting which may work best for different organizations regardless of the cloud provider. Once we finish up with network security, we'll spend a good amount of time discussing IAM core principles, as well as the service options available in each cloud provider. Then we'll start to assemble design structures for identity that include federation, roles, asset profiles, and the use of IAM as an isolation and segmentation tactic. We'll finish up with some discussion on the use of larger-scale network and identity designs that employ multiple virtual private clouds (VPCs) and cloud accounts.

Topics: Introduction to Cloud Security Architecture Principles; Amazon Web Services Frameworks: Well Architected and Cloud Adoption (more depth); Azure Cloud Adoption Framework and Cloud + Assessments (Azure Architecture Review, Cloud Journey Tracker, Governance Benchmark); Google 5 Principles for Cloud Native Architecture; Network Security Controls and Design; Network Security Architecture Models and Design; Identity and Access Management Core Controls and Policies; IAM Advanced Controls: Federation, Roles, Instance Profiles, Identity "Isolation"; Multi-VPC and Multi-Account Architecture and Strategies

SECTION 3: Cloud Security Architecture and Operations: Part 2

The third section of SEC545 continues our breakdown of controls and architecture considerations, starting with cloud workload security and operations management. We'll then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We'll also cover another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider's DR and continuity, and so this is covered as well. Additional topics will include cloud control plane assessment and architecture (touching on cloud security posture management), as well as a discussion of multi-cloud security architecture and controls.

Topics: Cloud Workload Security and Operations Architecture; Data Security Controls and Architecture; Availability Design and Architecture; DR+BCP Considerations; Cloud Control Plane Security (Cloud Security Posture Management); Multi-cloud Security Architecture

SECTION 4: Cloud Security Offense and Defense Operations

There are many threats to our cloud assets, so the fourth section of the course begins with an in-depth breakdown of the types of threats out there. We'll look at numerous examples. We'll also show you how to design a proper threat model focused on the cloud by using several well-known methods such as STRIDE and attack trees and libraries. On the defensive side, we start with network-based and host-based intrusion detection, and how to monitor and automate our processes to better carry out this detection. This is an area that has definitely changed from what we're used to in-house, so security professionals need to know what their best options are and how to get this done. We then cover incident response and forensics (also topics that have changed significantly in the cloud). The tools and processes are different, so we need to focus on automation and event-driven defenses more than ever. Scanning and pen testing the cloud used to be challenging due to restrictions put in place by the cloud providers themselves. But today we are seeing significant progress, with most mature solutions well adapted to cloud provider environments. There are some important points to consider when planning a vulnerability management strategy in the cloud, and we'll touch on how to best scan your cloud assets and which tools are available to get the job done. Pen testing naturally follows this discussion, so we'll talk about how to work with the cloud providers to coordinate tests as well as how to perform testing yourself.

Topics: Cloud Threats and Threat Modeling; Building Cloud Defensive Guardrails; Cloud Forensics and Incident Response; Cloud Vulnerability Assessment; Cloud Pen Testing + Red Team Operations

SECTION 5: Cloud Security Automation and Orchestration

In our final section, we'll focus explicitly on how to automate security in the cloud, both with and without scripting techniques. We will use tools like the AWS CLI and AWS Lambda to illustrate the premises of automation, then turn our attention to DevSecOps principles. We begin by explaining what that really means, and how security teams can best integrate into DevOps and cloud development and deployment practices. We'll cover automation and orchestration tools like Ansible and Chef, as well as how to develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from Section 4, we will look at event-driven detection and event management, as well as response and defense strategies that work. While we won't automate everything, some actions and scenarios really lend themselves to monitoring tools like CloudWatch, tagging assets for identification in security processes, and initiating automated response and remediation to varying degrees. We wrap up the course section covering a few more tools and tactics, followed by a sampling of real-world use cases.

Topics: Introduction to Automation and the AWS CLI; DevOps + DevSecOps Introduction (Pipeline Security); Infrastructure-as-Code; Systems Management and Orchestration; Automating Detection and Response; Final Tools and Considerations

Live Online sans.org/live-online

EVENT	START DATE
Cloud Defender	Jan 11
Cyber Security West: Feb	Feb 1
Scottsdale: Virtual Edition	Feb 22
Leadership & Cloud Security	Mar 29
Baltimore Spring: Virtual Edition	Apr 26
Cyber Security Central: May	May 3
Cyber Security East: May	May 17
CloudSec Next Summit	Jun 7

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

ICS410: **ICS/SCADA Security Essentials**

GICSP
Industrial Cyber Security Professional
giac.org/gicsp

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense (detecting host- and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, Center for Internet Security Critical Security Controls, and COBIT 5

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as ICS penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of ICS, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their ICS environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

> **"The course is informative and relevant to anyone working with or alongside industrial control systems."**
>
> — Abrael Delgado, **Compuquip Technologies**

ICS410: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: ICS Overview

Students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

Topics: Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Purdue Levels 0 and 1; Purdue Levels 2 and 3; IT & ICS Differences; Physical and Cybersecurity

SECTION 2: Architectures and Field Devices

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During Section 2, students will develop a better understanding of where these specific attack vectors exist and more defensible architectures for OT/ICS. Students will look at different technologies and communications used in Purdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from the PLCs they programmed in Section 1 and look at what other fieldbus protocols are used in the industry.

Topics: ICS Attack Surface; Secure ICS Network Architectures; Purdue Levels 0 and 1

SECTION 3: Communications and Protocols

Section 3 will take students through the communication protocols often found throughout control networks. Students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol. Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each.

Topics: Ethernet and TCP/IP; Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses

SECTION 4: Supervisory Systems

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. After a hands-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Purdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks. In the second half of the course section, students will learn how to create baselines and secure Windows-based workstation and servers.

Topics: Supervisory Servers; User Interfaces; Defending Microsoft Windows; Patching ICS Systems

SECTION 5: ICS Security Governance

Section 5 will further explore baselines and hardening, but this time on Linux-based workstations and servers. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Finally, students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments.

Topics: Defending Unix and Linux; Endpoint Protection and SIEMS; Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Measuring Cybersecurity Risk; Incident Response; Final Thoughts and Next Steps

SECTION 6: Capstone Exercise

Students will work through a group-based, table-top exercise (TTX) that includes hands-on components. Students must use the knowledge they gained throughout the week to identify indicators of compromise (IoCs), determine actions that should be taken to limit the attacker's ability to compromise additional assets, and react to changes in the attacker's tactics, techniques, and procedures (TTPs) as they progress deeper into the OT/OCS network. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

> **"Good comprehensive content with dynamic instructor really made this course good. This is the best training course I've taken in 25+ years."**
>
> — Curt Imanse, **Accenture**

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
Cyber Security West: Feb	Feb 1
ICS Summit	Mar 8
Baltimore Spring: Virtual Edition	Apr 26
Cyber Security Central: June	Jun 7

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

ICS456: **Essentials for NERC Critical Infrastructure Protection**

GCIP
Critical Infrastructure Protection
giac.org/gcip

5 Day Program	31 CPEs	Laptop Required

You Will Be Able To

- Understand the cybersecurity objectives of the NERC Critical Infrastructure Protection (CIP) standards
- Understand the NERC regulatory framework, its source of authority, and the process for developing CIP standards, as well as their relationship to the other Bulk Electric System (BES) reliability standards
- Speak fluent NERC CIP and understand how seemingly similar terms can have significantly different meanings and impacts on your compliance program
- Break down the complexity to more easily identify and categorize BES cyber assets and systems
- Develop better security management controls by understanding what makes for effective cybersecurity policies and procedures
- Understand physical and logical controls and monitoring requirements
- Make sense of the CIP-007 system management requirements and their relationship to CIP-010 configuration management requirements, and understand the multiple timelines for assessment and remediation of vulnerabilities
- Determine what makes for a sustainable personnel training and risk assessment program
- Develop strategies to protect and recover BES cyber system information
- Know the keys to developing and maintaining evidence that demonstrates compliance and be prepared to be an active member of the audit support team
- Sharpen your CIP Ninja!

This course empowers students with knowledge of the “what” and the “how” of the version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Reliability Corporation (NERC), and the Regional Entities, provides multiple approaches for identifying and categorizing Bulk Electric System (BES) cyber systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

The course features 25 hands-on labs range from securing workstations to digital forensics and lock picking.

The SANS ICS456: NERC Critical Infrastructure Protection Essentials course was developed by SANS ICS team members with extensive electric industry experience, including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC Critical Infrastructure Protection (CIP) Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

You Will Learn:

- BES cyber system identification and strategies for lowering their impact rating
- Nuances of NERC-defined terms and the applicability of CIP standards and how subtle changes in definitions can have a big impact on your program
- The significance of properly determining cyber system impact ratings and strategies for minimizing compliance exposure
- Strategic implementation approaches for supporting technologies
- How to manage recurring tasks and strategies for CIP program maintenance
- Effective implementations for cyber and physical access controls
- How to break down the complexity of NERC CIP in order to communicate with your leadership
- What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls
- How to understand the most recent Standards Development Team’s efforts and how that may impact your current CIP program

> **“This is best-in-class NERC CIP training. The courseware provides valuable compliance approaches and software tools for peer collaboration to build consent on implementation.”**
>
> — Jeff Mantong, **WAPA**

ICS456: **Section Descriptions**

Course Preview available at: **sans.org/demo**

SECTION 1: Asset Identification and Governance

A transition is under way from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. In Section 1, students will develop an understanding of the electricity sector regulatory structure and history as well as an appreciation for how the CIP standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES cyber asset identification and learn the critical role of strong management and governance controls. The section will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition that helps bring the concepts to life and highlights the important role we play in defending the grid.

Topics: Regulatory History and Overview; NERC Functional Model; NERC Reliability Standards; CIP History; Terms and Definitions; CIP-002: BES Cyber System Categorization; CIP-003: Security Management Controls

SECTION 2: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. During Section 2, we move beyond the “what” of CIP compliance to understanding the “why” and the “how.” Firewalls, proxies, gateways, IDS and more – we’ll learn where and when they help as well as learn practical implementations to consider and designs to avoid. Physical protections include more than fences and you’ll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce what is learned throughout the section and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

Topics: CIP-005: Electronic Security Perimeter(s); Interactive Remote Access; External Routable Communication and Electronic Access Points; CIP-006: Physical Security of BES Cyber Systems; Physical Security Plan; Visitor Control Programs; PACS Maintenance and Testing; CIP-014: Physical Security

SECTION 3: System Management

CIP-007 has consistently been one of the most violated standards going back to CIP version 1. With the CIP standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout Section 3, students will dive into CIP-007. We’ll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. This section will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We’ll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

Topics: CIP-007: System Management; Physical and Logical Ports; Patch Management; Malicious Code Prevention; Account Management; CIP-010: Configuration Change Management and Vulnerability Assessments; Change Management Program; Baseline Configuration Methodology; Change Management Alerting/Prevention

SECTION 4: Information Protection and Response

Education is key to every organization’s success with NERC CIP, and the students in ICS 456 will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, all students can be a valued resource to their organization’s CIP-004 training program, the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. In Section 4 we’ll examine CIP-008 and CIP-009 covering identification, classification, communication of incidents, and the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs in Section 4 will introduce tools for ensuring file integrity and sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

Topics: CIP-004: Personnel & Training; Security Awareness Program; CIP Training Program; PRA Evaluation Process; CIP-011: Information Protection; Information Protection Program; Data Sanitization; CIP-008: Incident Reporting and Response Planning; Incident Response Plan/Testing; Reporting Requirements; CIP-009: Recovery Plans for BES Cyber Systems; Recovery Plans; System Backup

SECTION 5: CIP Process

In the final section, students will learn the key components for running an effective CIP compliance program. We will review the NERC processes for standards development, the determination of penalties for violations, Requests For Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally we’ll identify recurring and audit-related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFEs, and self-reporting. We’ll also look at the challenge of preparing for NERC audits and provide tips to be prepared to demonstrate the awesome work your team is doing. Finally, we’ll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of Section 5, students will have a strong call to action to participate in the ongoing development of CIP within their organization and in the industry overall as well as a sense that CIP is doable! Labs in Section 5 will cover DOE C2M2, audit tools, and an audit-focused take on a blue team-red team exercise.

Topics: Scenario One:
CIP Processes for Maintaining Compliance; Preparing for an Audit; Audit Follow-Up; CIP Industry Activities; Standards Process; CIP of the Future

Who Should Attend

- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations personnel
- Incident response personnel
- Compliance staff
- Team leaders
- Persons involved in governance
- Vendors/Integrators
- Auditors

> **“This is a great course that examines NERC CIP standards and compliance from a variety of perspectives. I recommend it to anyone working with CIP.”**
>
> — Tom Duffey, **Accenture Security**

Live Online sans.org/live-online

EVENT	START DATE
Security East	Jan 11
ICS Summit	Mar 8
Cyber Security Central: June	Jun 7

OnDemand sans.org/ondemand

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

ICS515: **ICS Active Defense and Incident Response**

GRID
Response and Industrial Defense
giac.org/grid

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Analyze ICS-specific threats and take proper courses of action to defend the industrial control systems
- Establish collection, detection, and response strategies for your ICS networks
- Use proper procedures during ICS incident response

"ICS515 integrated the OT/ICS side of security into the course well, not like other courses I've taken that taught general IT security with OT added as an afterthought."

— Josh Tanski, **Morton Salt**

ICS515: ICS Active Defense and Incident Response will help you deconstruct industrial control system (ICS) cyber attacks, leverage an active defense to identify and counter threats to your ICS, and use incident response procedures to maintain the safety and reliability of operations.

The course will empower students to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense, which is needed to counter advanced adversaries targeting ICS, as has been seen with malware such as STUXNET, HAVEX, CRASHOVERRIDE, and TRISIS. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others.

The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing threat analysis and incident response to ensure the safety and reliability of operations. The strategic and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

This course will prepare you to:

- Perform ICS incident response focusing on security operations and prioritizing the safety and reliability of operations
- Understand how ICS threat intelligence is generated and how to use what is available in the community to support ICS environments. The analysis skills you learn will enable you to critically analyze and apply information from ICS threat intelligence reports on a regular basis
- Identify ICS assets and their network topologies and monitor ICS hotspots for abnormalities and threats. The course will introduce and reinforce methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape
- Analyze ICS threats and extract the most important information needed to quickly scope the environment and understand the nature of the threat
- Operate through an attack and gain the information necessary to instruct teams and decision-makers on whether operations must shut down or it is safe to respond to the threat and continue operations
- Use multiple security disciplines in tandem to leverage an active defense and safeguard an ICS, all reinforced with hands-on labs and technical concepts

"This course was like a catalyst. It not only boosted my knowledge about the threats facing ICS environments and provided me with a framework to actively defend these threats, it also inspired me to learn more."

— Srinath Kannan, **Accenture**

ICS515: **Section Descriptions**

Course Preview
available at:
sans.org/demo

SECTION 1: Threat Intelligence

Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), document tactics, techniques, and procedures (TTPs), and guide security teams to find threats in the environment. During this first course section students will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This section features five hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, visualizing the attack space, and ingesting threat intelligence reports to guide their practices over the rest of the labs in the course.

Topics: Case Study: STUXNET; Introduction to ICS Active Defense and Incident Response; Intelligence Life-Cycle and Threat Intelligence; ICS Cyber Kill Chain; Identifying and Reducing the Threat Landscape; Sharing and Consuming ICS Threat Intelligence

SECTION 2: Asset Identification and Network Security Monitoring

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach students to use tools such as Wireshark, TCPdump, CyberLens, ELSA, Bro, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and analyze the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

Topics: Case Study: HAVEX; ICS Asset and Network Visibility; ICS Network Security Monitoring – Collection; ICS Network Security Monitoring – Detection; ICS Network Security Monitoring – Analysis

SECTION 3: Incident Response

The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept of ICS active defense and requires that analysts safely acquire digital evidence while scoping the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but during this section students will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use these data to perform timely forensic analysis and create IOCs. In the previous section's labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.

Topics: Case Study: German Steelworks Attack; Incident Response and Digital Forensics Overview; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Memory Forensics and Identifying Capabilities; Integrated Timely Analysis

SECTION 4: Threat and Environment Manipulation

Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section's labs identified the infected HMI and gathered a sample of the APT malware. In this section's labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.

Topics: Case Study: BlackEnergy2; ICS Threat and Environment Manipulation Goals and Considerations; Analyzing Acquired Evidence; Case Study: Ukraine Power Grid Attack, 2015; Malware Analysis Methodologies; Case Study: CRASHOVERRIDE; Documenting Knowledge; Case Study: TRISIS

SECTION 5: Active Defense and Incident Response Challenge

This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.

Topics:

Scenario One:
Identify the Assets and Map the ICS Networks; Perform ICS Network Security Monitoring to Identify the Abnormalities; Execute ICS Incident Response Procedures into the SANS Cyber City Data Files; Analyze the Malicious Capability and Determine if the Threat Is an Insider Threat or a Targeted External Threat

Scenario Two:
Identify the Software and Information Present on the DCS; Leverage ICS Active Defense Concepts to Identify the Real-World Malware; Determine the Impact on Operations and Remediation Needs

Who Should Attend

- ICS Incident Response Team leads and members who want to learn how to safely respond to advanced threats in industrial control systems with a focus on combined and continued security
- ICS and Operations Technology Security Personnel who want to learn how to leverage an industrial control system active defense, including network security monitoring and threat intelligence
- IT security professionals who want to expand their knowledge into the industrial control system field with an understanding of ICS protocols, threats, and priorities
- Security Operations Center (SOC) team leads and analysts who want to learn how to monitor OT networks and industrial control system assets in an ICS SOC or dual IT/OT SOC
- ICS Red Teams and penetration testers who want to learn the latest in defense tactics in order to identify how they can better perform, and how they can better highlight areas for improvement in industrial control system networks
- Active defenders who want to challenge themselves to identify and respond to advanced targeted threats

Live Online **sans.org/live-online**

EVENT	START DATE
Security East	Jan 11
CTI Summit	Jan 25
ICS Summit	Mar 8
Baltimore Spring: Virtual Edition	Apr 26
Cyber Security Central: June	Jun 7

OnDemand **sans.org/ondemand**

Self-paced instruction with four months of access to course content, labs, and subject-matter-expert support.

What's New!

Courses in Development

SANS

We are continually developing new courses, so you can learn the latest tools and technologies to keep your organization secure.

BLUE TEAM & CYBER DEFENSE

SEC595 Data Science and Machine Learning for Security Professionals

This interactive course will teach security professionals how to use data science techniques to quickly write scripts to manipulate and analyze network and security data and ultimately uncover valuable insights from security data.

SEC513 Modern Linux Security for the Enterprise and Cloud

The concept for this course is to expand from securing a limited number of Linux-based systems, often done manually one system at a time, to securing hundreds or thousands of Linux-based systems and containers, commonly found in today's enterprise and cloud-based environments, using configuration management and automation.

OFFENSIVE OPERATIONS

SEC550 Active Defense – Cyberspace Trapping, Attack Disruption and Cyber Deception

This course will help you better understand attackers and their methods, develop new strategies for defending your network, and track and disrupt attackers.

SEC556 IoT Penetration Testing

This course will immerse students into the interfaces commonly observed in IoT devices and provide a process and testing framework (IoTA) to evaluate these devices within many layers of the OSI model.

SEC565 Red Team Operations

This course prepares operators to emulate adversaries and threats in a professional manner to test a target organization's people, process, and technology from a holistic perspective.

DFIR

FOR509 Cloud Forensics & Incident Response

This course focuses on understanding forensic data in the cloud, implementing best practices, and conducting proper evidence preservation and memory acquisition in the cloud.

FOR710 Reverse-Engineering Malware: Advanced Code Analysis

This course continues where FOR610 leaves off, helping students who have already attained intermediate-level malware analysis capabilities take their reversing skills to the next level.

SECURITY MANAGEMENT

MGT416 Vendor Risk Management & Data Privacy

This course will provide an overview of the key elements that are required to properly implement and deliver a successful Vendor Risk and Data Privacy program.

CLOUD SECURITY

SEC388 Introduction to Cloud Computing and Security

This course steps through the many facets of the cloud. That includes establishing your very own cloud account in which you will explore the "Big Three" (Amazon Web Services, Azure, and Google Cloud Platform) cloud vendors of your choice, and exploring services to enhance operations, maintenance. We'll also cover some of the newer technologies where the cloud really shines (such as Infrastructure as Code and Serverless).

SEC557 Continuous Automation for Enterprise and Cloud Compliance

This course equips students to conduct more thorough and accurate assessments of cloud and enterprise systems and environments to increase the overall security posture.

Get More Information – Interested in new courses, certifications, and major course updates? Learn more and receive notifications at **sans.org/new-sans-courses**

RETURN TO TABLE OF CONTENTS

Change user behavior, mature your program, and protect your organization.

SANS SECURITY AWARENESS

End-User

EndUser training is available in 33 languages. Customize your program with our broad library of training modules and styles. Deliver training in our world-class Learning Management System, or your own.

Developer

Security by design starts here. Developer training ensures your entire team creates web applications in a secure environment, and places the best security protection in the right place.

Phishing

Test your team's readiness and awareness to respond to phishing attacks. Our Phishing platform supports a broad set of simulations, reports to identify risky behavior, and features to automatically assign training based on results.

Insights

Risk Measured is Risk Managed. Surface the insights you need to make informed decisions on your awareness program. The Insights Suite will help you measure program efficacy, reduce training costs, and train to your unique needs, all based on measuring risk.

sans.org/security-awareness-training

How to Get Started in Cybersecurity

Cybersecurity is a rapidly growing field where the demand for skilled professionals is far outpacing supply. If you are interested in a cybersecurity career, SANS is the place to learn the foundations of cybersecurity to help you get started.

COURSES

The Best FREE Online Cybersecurity Course

SANS Cyber Aces

SANS Cyber Aces is an online course that teaches the core concepts needed to assess and protect information security systems.
cyberaces.org

Brand New to Computers

SANS Foundations

Learn the core knowledge and practical skills in computers, technology, and security fundamentals that will kickstart your career in cybersecurity.
sans.org/sans-foundations

New to Cybersecurity

SEC301: Introduction to Cyber Security

This entry-level certification course is the fastest way to get up to speed in InfoSec.
sans.org/sec301

New to InfoSec with Some IT Background

SEC401: Security Essentials Bootcamp Style

SEC401 provides you the essential InfoSec skills and techniques you need to protect and secure your organization's critical information and technology assets.
sans.org/sec401

FREE RESOURCES

CyberStart

Prepare to become a code-breaking, password-cracking, and ethical-hacking cyber detective with CyberStart.
cyberstart.com

Cyber Camp

Cyber Camp is an event geared towards high school or junior high students interested in computers and cybersecurity.
sans.org/cyber-camp

◀ RETURN TO TABLE OF CONTENTS

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

The most trusted source for cybersecurity training, certifications, degrees, and research

Free Cybersecurity Resources

SANS instructors and analysts produce thousands of free resources and tools for the cybersecurity community, including more than **150 free tools and hundreds of white papers authored annually.** SANS remains committed to providing free education and capabilities to the cyber communities we serve, train, and certify.

Free Cybersecurity Community Resources

- **Internet Storm Center –** Free Analysis and Warning Service
- **White Papers –** Community InfoSec Research
- **Blog –** Cybersecurity Blog
- **Newsletters –** Newsbites; @Risk; OUCH!
- **Webcasts –** Live and Archived
- **Posters –** Job-Focused Resources
- **SANS Holiday Hack Challenge**
- **Critical Security Controls –** Recommended Actions for Cyber Defense
- **Podcasts –** Internet Storm Center Daily Stormcast; Trust Me, I'm Certified; Blueprint

SANS Faculty Free Tools

SANS Instructors have built more than 150 open-source tools that support your work and help you implement better security.

Free Training and Events

- ▶ **Test Drive 45+ SANS Courses**
- ▶ **Capture-the-Flag Cyber Challenges**
- ▶ **Cyber Aces**
- ▶ **Free SANS Summits & Forums**

sans.org/free

◀ RETURN TO TABLE OF CONTENTS