The most trusted source for information security training, certification, and research

Cybersecurity Training and Certifications

2019 Catalog

100+ extraordinary SANS-certified instructors

300+ training events, plus multiple online options

Curricula

Cyber Defense
Detection and Monitoring
Penetration Testing
Incident Response
Digital Forensics

Ethical Hacking
Management, Audit, Legal
DevSecOps
Cyber Threat Intelligence
ICS/SCADA Security

“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.

www.sans.org

Summer/Fall
SANS Institute

The most trusted source for information security training, certification, and research

At the SANS Institute, our mission is to deliver the cutting-edge information security knowledge and skills that companies, military organizations, and governments need to protect their people and assets.

TRAINING ON THE CUTTING EDGE
SANS offers more than 65 unique courses, all designed to align with dominant security team roles, duties, and disciplines. Our courses prepare students to face today’s threats and tomorrow’s challenges.


In SANS courses, students are immersed in hands-on lab exercises designed to help them practice, hone, and perfect what they’ve learned. And we constantly update and rewrite our courses to be sure the tools and techniques we’re teaching are always current, and on the cutting edge.

LEARN FROM THE BEST
The SANS faculty is simply unmatched. All of our instructors are active security practitioners, bringing their extensive knowledge and real-world experiences directly to the classroom.

SANS instructors work for high-profile organizations as red team leaders, CISOs, technical directors, and research fellows. In addition to their respected technical credentials, they’re also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom—both live and online—dynamic and effective.

GIAC CERTIFICATION
GIAC certifications are designed to ensure that students can apply their knowledge and skills in a real-world setting. More than 30 certifications align with SANS training courses, validating student mastery for professional use in critical, specialized InfoSec domains and job-specific roles. See www.giac.org for more information.

A TRAINING FORMAT FOR EVERY STUDENT
SANS holds more than 300 live training events around the world each year, so you can find a convenient time and place to take your course. These events provide an engaging learning environment and multiple opportunities to network with other security professionals and with SANS instructors and staff.

SANS training is also offered online, with several convenient options to suit your learning style. All of our online courses include at least four months of access to the course material, so students can revisit and rewind content anytime, anywhere.

RECOGNIZED AS A SUPERIOR INVESTMENT
Information security professionals from every member of the Fortune 100, and from small and mid-sized firms alike, say they return to SANS training again and again because they trust their training will result in practical and high-quality capabilities. SANS training is also embedded in government and military programs in the United States and allies around the world for the same reason.

Customer feedback drives our continuous effort to maintain the quality and impact of SANS training, so that we continue to deserve your trust.

THE SANS PROMISE
At the heart of everything we do is the SANS Promise: Students will be able to use their new skills as soon as they return to work.

REGISTER FOR SANS TRAINING
Learn more about SANS courses, and register online, at www.sans.org

The SANS suite of education resources for information security professionals includes:

- SANS Training: Live & Online
- GIAC Certifications
- NetWars Experience
- Security Awareness
- Internet Center
- CyberTalent
Table of Contents

2 The SANS Faculty
3 Build a High-Performing Security Organization
4 SANS Training Roadmap
5 SANS Training Formats
6 Securing Approval and Budget for Training
7 GIAC Certifications
8 SANS Flagship Programs and Free Resources
9 SANS Security Awareness
10 SANS Technology Institute
11 SEC401 Security Essentials Bootcamp Style
12 SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling
13 MGT512 Security Leadership Essentials for Managers | NEW
14 SEC566 Implementing and Auditing the Critical Security Controls – In-Depth
15 SEC503 Intrusion Detection In-Depth
16 SEC511 Continuous Monitoring and Security Operations
17 SEC301 Introduction to Cyber Security
18 SEC487 Open-Source Intelligence (OSINT) Gathering and Analysis | NEW
19 SEC505 Securing Windows and PowerShell Automation
20 SEC506 Securing Linux/Unix
21 SEC501 Advanced Security Essentials – Enterprise Defender
22 SEC530 Defensible Security Architecture and Engineering | NEW
23 SEC545 Cloud Security Architecture and Operations
24 SEC555 SIEM with Tactical Analytics
25 SEC599 Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses
26 SEC560 Network Penetration Testing and Ethical Hacking
27 SEC542 Web App Penetration Testing and Ethical Hacking
28 SEC460 Enterprise Threat and Vulnerability Assessment | NEW
29 SEC573 Automating Information Security with Python
30 SEC575 Mobile Device Security and Ethical Hacking
31 SEC617 Wireless Penetration Testing and Ethical Hacking
32 SEC642 Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
33 SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
34 SEC760 Advanced Exploit Development for Penetration Testers

60 FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics | NEW
61 FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | NEW
62 FOR500 Windows Forensic Analysis
63 FOR518 Mac and iOS Forensic Analysis and Incident Response
64 FOR526 Advanced Memory Forensics & Threat Detection
65 FOR578 Cyber Threat Intelligence
66 FOR585 Smartphone Forensic Analysis In-Depth
67 FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
68 MGT414 SANS Training Program for CISSP® Certification
69 MGT514 Security Strategic Planning, Policy, and Leadership
70 MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep
71 AUD507 Auditing & Monitoring Networks, Perimeters, and Systems
72 LEG523 Law of Data Security and Investigations
73 DEV522 Defending Web Applications Security Essentials
74 SEC540 Cloud Security and DevOps Automation
75 DEV541 Secure Coding in Java/JEE: Developing Defensible Applications
76 DEV544 Secure Coding in .NET: Developing Defensible Applications
77 ICS410 ICS/SCADA Security Essentials
78 ICS456 Essentials for NERC Critical Infrastructure Protection
79 ICS515 ICS Active Defense and Incident Response
80 Cyber Defense 2-Day & Beta Courses
81 Penetration Testing 2-Day Courses
82 IR & Forensics Beta Course
83 DevSecOps 2-Day Course
84 Management 2-Day & Beta Courses
85 Hosted Courses
86 SANS Voucher Program
87 SANS NetWars Experience
88 Upcoming Summit & Training Events

“SANS courses give you real-world skills that have an immediate value on the security environment.”

– Eric Kaithula, Symetra
**SANS Faculty**

“SANS instructors are the best in the game. Their technical knowledge combined with presentation skills and real-world examples make for an unparalleled training experience. SANS rocks!”

- Chris Gergen, Bank of North Dakota

At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge by drawing on their own their own real-world examples and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 100 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organizations around the world.

In addition to their impressive résumés, every member of the SANS faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they’re present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you’ll be able to apply what you learn from these top-tier instructors as soon as you return to work.

Meet the SANS faculty: [www.sans.org/instructors](http://www.sans.org/instructors)
Based on our global research, SANS has identified effective strategies for building an information security group:

**Use practical organizing principles** to design your plan. Nearly all of the more complex frameworks may be reduced to a few simpler constructs, such as “Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents.”

**Prioritize** your efforts within these areas, using the Center for Internet Security Critical Controls, as you mature your own organization.

**Determine the number and types of professionals you need** to perform the hands-on work, then **launch an ongoing campaign** to develop a team with the appropriate skills in mind. Cybersecurity is a specialized practice area within IT, and demands specialized training.

The job roles and skills required in information security grow and change as the organization scales. While every professional needs a baseline of knowledge and capabilities in cyber defense and incident response, over time you will develop specialized members of your team to work together in particular areas.

Four critical job roles typically emerge:

- **Security Monitoring & Detection Professionals** – Identifying security anomalies within your environment requires an increasingly sophisticated set of skills. All too often, vendor training teaches to the tool, without explaining how the tool works or how it can be best used. To deploy detection and monitoring tools and interpret their output, you need a more robust understanding of tools, techniques, and analysis.

- **Pen Testers & Vulnerability Analysts** – A professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different set of tools and a different way of thinking, but it’s still essential in improving defenses.

- **Forensic Investigators & Incident Responders** – Larger organizations need specialized professionals who can move beyond first-level incident response. Whether you’re maintaining a trail of evidence or hunting for threats, you need the skills to analyze attacks and develop appropriate remediation and recovery plans.

- **Security Managers** – As their staffs of talented technologists grow, organizations require effective leaders to manage them. These managers won’t necessarily perform hands-on work, but they must understand enough about underlying technologies and frameworks to help set security strategy, develop appropriate policies, interact with their skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, a high-performing security organization will develop individuals further, with some individual professionals able to cover more areas, while others go deeper into just one specialty. Along the entire spectrum from active defense to cloud defense, and from Python for InfoSec professionals to malware reengineering, SANS offers more than 30 courses to train for specialized roles or learn about more advanced topics, meeting the needs of security professionals at every level.
You are a candidate for specialized or advanced training.

Cyber Defense Operations

<table>
<thead>
<tr>
<th>Specialized Defense Area</th>
<th>Hardened Specific Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Emulation</td>
<td>GIAC Certified Advanced Emulation Defender</td>
</tr>
<tr>
<td>Clinical Security</td>
<td>GIAC Certified Clinical Security Defender</td>
</tr>
<tr>
<td>Windows or Server</td>
<td>GIAC Certified Windows or Server Professional</td>
</tr>
<tr>
<td>Linux/Unix Security</td>
<td>GIAC Certified Linux/Unix Defender</td>
</tr>
<tr>
<td>SWK</td>
<td>GIAC Certified SWK with Tactical Analytics</td>
</tr>
</tbody>
</table>

Other Advanced Defense Courses

<table>
<thead>
<tr>
<th>Advanced Defense Courses</th>
<th>Specialized Defensive Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Architecture</td>
<td>GIAC Certified Security Architecture and Engineering</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>GIAC Certified Defending Advanced Adversaries – Purple Team Tactics and Red Team Defense</td>
</tr>
</tbody>
</table>

Specialized Penetration Testing

<table>
<thead>
<tr>
<th>In-Depth Coverage</th>
<th>Focused Techniques and Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Assessment</td>
<td>GIAC Certified Enterprise Threat and Vulnerability Assessment</td>
</tr>
<tr>
<td>Networks</td>
<td>GIAC Certified Advanced Penetration Testing, Exploitation, and Intrusion Testing</td>
</tr>
<tr>
<td>Web Apps</td>
<td>GIAC Certified Advanced Web App Penetration Testing, Exploitation, and Exploitation Techniques</td>
</tr>
<tr>
<td>Mobile</td>
<td>GIAC Certified Mobile Devices Security and Ethical Hacking</td>
</tr>
<tr>
<td>Wireless</td>
<td>GIAC Certified Wireless Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>Python Coding</td>
<td>GIAC Certified Automating Information Security with Python</td>
</tr>
</tbody>
</table>

Digital Forensics, Malware Analysis, & Threat Intel

<table>
<thead>
<tr>
<th>Specialized Investigation Skills</th>
<th>Malware Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Analysis</td>
<td>GIAC Certified Reverse Engineering Malware: Malware Analysis Tools and Techniques</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>GIAC Certified Cyber Threat Intelligence</td>
</tr>
<tr>
<td>Digital Forensics &amp; Malware Exploitation</td>
<td>GIAC Certified Digital Forensics &amp; Malware Exploitation</td>
</tr>
<tr>
<td>Memory Forensics</td>
<td>GIAC Certified Advanced Memory Forensics</td>
</tr>
<tr>
<td>Malware Forensics</td>
<td>GIAC Certified Malware Forensics and Memory Forensics</td>
</tr>
</tbody>
</table>

Advanced Management

<table>
<thead>
<tr>
<th>Advanced Leadership, Audit, Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Skills</td>
</tr>
<tr>
<td>Project Management</td>
</tr>
<tr>
<td>Audit &amp; Legal</td>
</tr>
<tr>
<td>Law &amp; Investigations</td>
</tr>
</tbody>
</table>
SANS Training Formats

You can take SANS courses when, where, and how you want—regardless of your training path. Whether you opt for a live event or one of our many online options, your SANS training experience will always exceed expectations.

Live Classroom Instruction

Training Events
Our live events feature SANS instructors teaching multiple courses at a single location. You'll get:
- Focused, immersive learning without distractions
- Direct access to SANS Certified Instructors
- Opportunities to network with and learn from other cybersecurity professionals
- The chance to attend SANS@Night events, NetWars, vendor presentations, industry receptions, and many other activities

Our live events in North America serve thousands of students annually in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Smaller, regional events are scheduled in most major metropolitan areas throughout the year.

Summits
SANS Summits take place over one or two days, and focus on a single topic of particular interest to the community. We curate our presentations and speakers to ensure that participants get the most relevant and applicable information.
Before or after each Summit we offer SANS courses that are closely aligned with the topic, so you can enhance your Summit experience with in-depth training while you’re there.

Community SANS Courses
Our Community events offer SANS courses, courseware, and labs taught by up-and-coming instructors in more local, regional areas.
With smaller classes, you get more direct interaction with your instructor, and the regional location means an easier, less expensive commute.

Private Classes
A SANS Certified Instructor can train your staff privately at your location, incorporating insights, stories, and questions specific to your business objectives.
Private training allows your team to freely discuss sensitive issues, and spend more time focusing on the topics most relevant to your organization.

Online Training

SANS Online Training features course authors and top instructors teaching our most popular courses, delivered via four flexible online platforms:
- OnDemand: Learn anytime, anywhere with our custom OnDemand platform
- vLive: Attend virtual evening sessions with SANS instructors
- Simulcast: Livestream a daytime SANS course from a live event
- SelfStudy: Self-paced learning with books and MP3s

Our online training platforms include either four or six months of access to your course, as well as support from a team of SANS subject-matter experts. Access to all course labs and the ability to revisit content without limits ensures that you can master the content at your own pace.
Because you can rewind, revisit, and reinforce the course material, retention is easier and your learning outcome will be the same as if you attended live SANS training. Try out the OnDemand platform by viewing a course preview at www.sans.org/demo.

“The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life.”
-Dan Trueman, Novae PLC

“I love the material, I love the SANS Online delivery, and I want the entire industry to take these courses.”
-Nick Sewell, IIT
Securing Approval and Budget for Training

As a cybersecurity professional, you already know that SANS is the most trusted resource for the training you need. But getting buy-in from your manager or the C-Suite can be a challenge—especially if they don’t already understand the benefits that SANS training can bring. By following some simple guidelines, you can show them what they need to see, and get them to support your training.

Packaging matters

Submit a formal request

- Most successful training requests are made via written document—a short memo or a few PowerPoint slides—justifying the need for training. Training request templates are available for popular SANS courses. They can be found in the “Justify Your Training” section of the course page. Most managers will respect and value the effort you put in to provide written justification.

- A formal request is a chance for you to provide all the necessary information in one place. If you include additional SANS resources, you can give your manager context and present your request as a complete package. Some helpful additions include the Why SANS? web page, the Training Roadmap, an instructor bio, and a course description.

Clearly state the benefits

Be specific

- How does the course relate to your job? Will it help you establish baseline skills? Transition to a more focused role? Decision-makers need to understand the plan.

- Highlight specific tasks you’ll be able to do as a result of the training. Each SANS course description includes a section titled “You Will Be Able To;” include this section in your request to make the benefits clear. Match the training to your job tasks and goals.

Set the context

Establish long-term expectations

- Cybersecurity is a specialized career path within IT. Its practices evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of team salaries to keep skills current. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.

- Sign up for the related GIAC certification, in order to validate that you learned the skills taught in the class. Your employer can be confident you learned what they paid for, since GIAC exams are psychometrically designed to confirm competency in job-related tasks.

- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements when they’re hired; some offer to stay for a year after they complete the training.
Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC’s on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

“Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it’s a continuous fight.”

– Jason Sevilla, Cyber Intelligence Analyst

“Earning 3 GIAC certifications after I graduated from college has enabled me to enter the InfoSec field. Not only did they set me apart from my peers, GIAC certs also made my resume more appealing to recruiters.”

– Kim Ngoc, GuardSight, Inc.
Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge
Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design
The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

“Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it's a continuous fight.”
– Jason Sevilla, Cyber Intelligence Analyst

“Earning 3 GIAC certifications after I graduated from college has enabled me to enter the InfoSec field. Not only did they set me apart from my peers, GIAC certs also made my resume more appealing to recruiters.”
– Kim Ngoc, GuardSight, Inc.
Security Awareness Is Critical in Protecting Your Organization

What’s in your training content?

**Expert Led**

SANS awareness training content is built by the world’s leading cybersecurity practitioners. Cognitive experts, design theory animators, and leading security awareness experts deliver training content that protects your organization, and changes human behaviors.

**Relevant**

Our content is constantly updated to match current threats. Training is available in multiple formats, with a variety of supplemental materials, to reach every audience in any language.

**Easy**

Modules are created to match important threats, designed in core and specialized training module-sets to cover all aspects of training.

World-class training offered from top experts, all available in a variety of formats, and prepared for a global audience. Let SANS Security Awareness training help you manage human risk.

Learn more at: sans.org/security-awareness

“Whether for our developers, administrators, or executives, the SANS Security Awareness training curriculum hits the nail on the head! I can’t begin to count how many conversations have been sparked, relevant questions have been asked, light bulbs of understanding have lit up, and less secure behaviors have changed as a result of this content.”

Jim Raub, CISO and Vice President, EagleDream Technologies
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 7 months.

Flexibility
Pursue the certificate alongside undergraduate studies or while working full-time. Take courses online or at immersive weeklong events throughout the country.

“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

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.

Learn more at sans.edu/acs
SEC401: Security Essentials Bootcamp Style

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can 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?

If you do not know the answers to these questions, then SEC401 will provide the information security training you need in a bootcamp-style format that is 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 teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. Our course will show you how to prevent your organization’s security problems from being 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?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.
DAY 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 on this first day in order to provide a firm foundation for the consecutive days of training.

Topics: Defensible Network Architecture; Virtualization and Cloud Security; Network Device Security; Networking and Protocols; Securing Wireless Networks; Securing Web Communications

DAY 2: Defense-In-Depth and Attacks
To secure an enterprise network, you must understand the general principles of network security. On Day 2, we look at threats to our systems and take a “big picture” look at how to defend against them. You will learn that protections needed to be layered — a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.

Topics: Defense-in-Depth; Access Control and Password Management; Security Policies; Critical Controls; Malicious Code and Exploit Mitigations; Advanced Persistent Threat (APT)

DAY 3: Threat Management
Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems, mapping out networks, and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.

Topics: Vulnerability Scanning and Penetration Testing; Network Security Devices; Endpoint Security; SIEM/Log Management; Active Defense

DAY 4: Cryptography, Risk Management, and Response
There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. This course section looks at various aspects of encryption and how it can be used to secure a company’s assets. A related area called steganography, or information hiding, is also covered.

Topics: Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Incident Handling and Response; Contingency Planning – BCP/DRP; IT Risk Management

DAY 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 (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it 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, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section 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 day with a solid grounding in Windows security by looking at automation, auditing and forensics.

Topics: Windows Security Infrastructure; Service Packs, Hot Fixes, and Backups; Windows Access Controls; Enforcing Security Policy; Securing Windows Network Services; Automation, Auditing, and Forensics

DAY 6: Linux Security
While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final course day provides step-by-step guidance to improve the security of any Linux system. The course combines practical “how to” instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

Topics: Linux Security: Structure, Permissions and Access, 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 specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

Community Events
Tampa, FL ................................... Jun 10-15
Ottawa, ON .................................. Jul 8-13
Raleigh, NC ................................. Aug 12-17
Vancouver, BC ............................. Sep 23-28

Mentor Events
Austin, TX ..................................... Jun 1-29

Private Training
This course is also available through Private Training.

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

vLive
Online Training .............................. Sep 3 - Oct 10

Simulcast
Online Training .............................. Jun 17-22
Online Training .............................. Jul 8-13
Online Training .............................. Aug 12-17
Online Training .............................. Sep 9-14
SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**

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 lsqf 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 Nettac 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.
- 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 lsqf 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 Nettac 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.

“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 is available via (subject to change):**

**Live Training**

<table>
<thead>
<tr>
<th>City</th>
<th>City, State</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kansas City</td>
<td>Kansas City, MO</td>
<td>Jun 10-15</td>
</tr>
<tr>
<td>Charlotte</td>
<td>Charlotte, NC</td>
<td>Jul 8-13</td>
</tr>
<tr>
<td>Pittsburgh</td>
<td>Pittsburgh, PA</td>
<td>Jul 8-13</td>
</tr>
<tr>
<td>Rocky Mountain</td>
<td>Denver, CO</td>
<td>Jul 15-20</td>
</tr>
<tr>
<td>Columbia</td>
<td>Columbia, MD</td>
<td>Jul 15-20</td>
</tr>
<tr>
<td>San Francisco Summer</td>
<td>San Francisco, CA</td>
<td>Jul 22-27</td>
</tr>
<tr>
<td>Boston Summer</td>
<td>Boston, MA</td>
<td>Jul 29 - Aug 3</td>
</tr>
<tr>
<td>Crystal City</td>
<td>Arlington, VA</td>
<td>Aug 5-10</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Aug 12-17</td>
</tr>
<tr>
<td>Chicago</td>
<td>Chicago, IL</td>
<td>Aug 19-24</td>
</tr>
<tr>
<td>Virginia Beach</td>
<td>Virginia Beach, VA</td>
<td>Aug 25-30</td>
</tr>
<tr>
<td>New York City</td>
<td>New York, NY</td>
<td>Aug 25-30</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 9-14</td>
</tr>
<tr>
<td>Raleigh</td>
<td>Raleigh, NC</td>
<td>Sep 16-21</td>
</tr>
<tr>
<td>N. VA Fall – Reston</td>
<td>Reston, VA</td>
<td>Sep 30 - Oct 5</td>
</tr>
<tr>
<td>Baltimore Fall</td>
<td>Baltimore, MD</td>
<td>Oct 7-12</td>
</tr>
<tr>
<td>San Diego</td>
<td>San Diego, CA</td>
<td>Oct 7-12</td>
</tr>
<tr>
<td>Seattle Fall</td>
<td>Seattle, WA</td>
<td>Oct 14-19</td>
</tr>
<tr>
<td>Denver</td>
<td>Denver, CO</td>
<td>Oct 14-19</td>
</tr>
<tr>
<td>Santa Monica</td>
<td>Santa Monica, CA</td>
<td>Oct 21-26</td>
</tr>
<tr>
<td>Houston</td>
<td>Houston, TX</td>
<td>Oct 28 - Nov 2</td>
</tr>
<tr>
<td>DFRICON Miami</td>
<td>Coral Gables, FL</td>
<td>Nov 4-9</td>
</tr>
<tr>
<td>Atlanta Fall</td>
<td>Atlanta, GA</td>
<td>Nov 18-23</td>
</tr>
<tr>
<td>Austin</td>
<td>Austin, TX</td>
<td>Nov 18-23</td>
</tr>
<tr>
<td>Nashville</td>
<td>Nashville, TN</td>
<td>Dec 2-7</td>
</tr>
<tr>
<td>San Francisco Winter</td>
<td>San Francisco, CA</td>
<td>Dec 2-7</td>
</tr>
<tr>
<td>CDI</td>
<td>Washington, DC</td>
<td>Dec 14-19</td>
</tr>
</tbody>
</table>

**Summit Events**

- Security Operations | New Orleans, LA | Jun 26 - Jul 1
- THIR | New Orleans, LA | Oct 2-7
- Pen Test HackFest | Bethesda, MD | Nov 20-25

**CDI**

Washington, DC
Course Day Descriptions

**DAY 1: Incident Handling Step-by-Step and Computer Crime Investigation**
The first part of this section looks at the invaluable Incident Handling Step-by-Step Model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

**Topics:** Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record-Keeping; Incident Follow-Up

**DAY 2: Computer and Network Hacker Exploits – Part 1**
Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

**Topics:** Reconnaissance; Scanning; Intrusion Detection System (IDS) Evasion

**DAY 3: Computer and Network Hacker Exploits – Part 2**
Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course day covers the third phase of many hacker attacks — gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

**Topics:** Network-Level Attacks; Gathering and Parsing Packets; Operating System and Application-Level Attacks; Netcat: The Attacker’s Best Friend

**DAY 4: Computer and Network Hacker Exploits – Part 3**
This course day starts out by covering one of attackers’ favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations’ homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

**Topics:** Password Cracking; Web Application Attacks; Denial of Service Attacks

**DAY 5: Computer and Network Hacker Exploits – Part 4**
This course day covers the fourth and fifth phases of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens, as well as explore future trends in malware, including BIOS-level and combo malware possibilities.

**Topics:** Maintaining Access; Covering the Tracks; Putting It All Together

**DAY 6: Hacker Tools Workshop**
Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

**Topics:** Hands-on Analysis

---

**Community Events**
- Santa Monica, CA .............................. Jun 24-29
- Madison, WI ................................. Jul 8-13
- Colorado Springs, CO ........................... Jun 17-22
- Phoenix, AZ ................................. Sep 23-28

**Mentor Events**
- Santa Monica, CA ............................. Jun 5 - Jul 17
- Austin, TX ................................. Jun 13 - Aug 8

**Private Training**
This course is also available through Private Training.

**Online Training**
- OnDemand
  - Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
- vLive
  - Online Training .......................... Aug 13 - Sep 19
  - Online Training ............................ Nov 5 - Dec 19

**Simulcast**
- Online Training ............................. Jun 17-22
- Online Training .............................. Jul 8-13
- Online Training ............................. Sep 9-14
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.

To accomplish this goal, 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. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues.

This approach prepares 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
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud

MGT512 uses case studies, group discussions, team-based exercises, and in-class games to help students absorb both technical and management topics.
Course Day Descriptions

**DAY 1: Building Your 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

**DAY 2: Protecting Data and Networks**
Day 2 provides foundational knowledge to protect data and networks. This includes building an understanding of cryptography concepts, encryption algorithms, and applications of cryptography. Since encrypting data alone is not sufficient, the distinction between privacy and security is discussed to give managers a primer on key privacy concepts. Finally, a thorough discussion of network security is modeled around the various layers of the network stack. This allows managers to gain a deeper understanding of what their teams are talking about, what vendors are selling, and where various issues and protections lay within the seven layers of the network model.

**Topics:** Data Protection; Privacy Primer; Network Security

**DAY 3: Protecting and Patching Systems**
Day 3 is focused on protecting and patching systems. This includes coverage of host security that encompasses endpoint and server security along with malware and attack examples. Modern infrastructure as code approaches and tools are also discussed as ways to automate consistent deployment of standard configurations. Managers must also be knowledgeable about software development processes, issues, and application vulnerabilities. Coverage includes an overview of the secure SDL, OWASP Top Ten, and leading-edge development processes built on DevOps. Managers must also understand physical security controls that, when not implemented appropriately, can cause technical security controls to fail or be bypassed. All of these issues and corresponding vulnerabilities must be appropriately managed. This leads to a discussion on building a vulnerability management program and the associated process for successfully finding and fixing vulnerabilities.

**Topics:** Host Security; Application Security; Physical Security; Vulnerability Management

**DAY 4: Leading Modern Security Initiatives**
Day 4 covers what managers need to know about leading modern security initiatives. Security awareness is a huge component of any security program that is focused on driving activities that lead to changes in human behavior and creating a more risk-aware and security-aware culture. 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. The cloud is a major initiative that many organizations are either tackling now or planning to undertake. To get ready for these initiatives, an overview of Amazon Web Services (AWS) is provided to serve as a reference, along with a discussion of 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. To execute such new initiatives security leaders must also develop negotiation skills and the ability to manage highly technical team members.

**Topics:** Security Awareness; Project Management; Cloud Security; Modern Security Architecture; Management Methods

“MGT512 is valuable because it is relevant/current to the security landscape from my management vantage point.”

--Michael Bradley, Prudential Financial
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.

“SEC566 provides great tools, explanation, and insight!”
-Ryan LeVan, Trex Company, Inc.
DAY 1: Introduction and Overview of the 20 Critical Controls

Day 1 will introduce you to all of the Critical Controls, laying the foundation for the rest of the class. For each Control, we will follow the same outline covering the following information:

- Overview of the Control
- How It Is Compromised
- Defensive Goals
- Quick Wins
- Visibility & Attribution
- Configuration & Hygiene
- 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

DAY 2: Critical 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

DAY 3: Critical 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

DAY 4: Critical Controls 12, 13, 14, and 15

Topics: Critical Control 12: Boundary Defense; Critical Control 13: Data Protection; Critical Control 14: Controlled Access Based on the Need to Know; Critical Control 15: Wireless Device Control

DAY 5: Critical 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)

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

“...understand why the Controls are necessary for securing systems at my organization.”

-Brandon McWilliams, SRP

Online Training

OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

Simulcast
Online Training ............................. Jun 17-21
Online Training ............................. Aug 12-16
Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

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 different open-source tools like tcpdump, Wireshark, Snort, Bro, 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. 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 VM is provided with tools of the trade. It is supplemented with demonstration “pcaps,” which are files that contain network traffic. This allows you to follow along on your laptop with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

SEC503 is most appropriate for persons who monitor and defend their network, such as security analysts, although others may benefit from the course as well. Students range from seasoned analysts to novices with some TCP/IP background. Please note that the VMware image used in class is a Linux distribution, so we strongly recommend that you spend some time getting familiar with a Linux environment that uses the command line interface. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

SEC503 is most appropriate for persons who monitor and defend their network, such as security analysts, although others may benefit from the course as well. Students range from seasoned analysts to novices with some TCP/IP background. Please note that the VMware image used in class is a Linux distribution, so we strongly recommend that you spend some time getting familiar with a Linux environment that uses the command line interface. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.
### Course Day Descriptions

**DAY 1: Fundamentals of Traffic Analysis – Part 1**
Day 1 provides a refresher or introduction, depending on your background, to TCP/IP. It describes the need to understand packet structure and content. It covers the essential foundations such as the TCP/IP communication model, and the theory of bits, bytes, binary and hexadecimal. We introduce the use of open-source Wireshark and tcpdump for analysis. We begin our exploration of the TCP/IP communication model with the study of the link layer, the IP layer, both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender. All traffic is discussed and displayed using the two open-source tools, Wireshark and tcpdump.

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

---

**DAY 2: Fundamentals of Traffic Analysis – Part 2**
Day 2 continues where the previous day ended in understanding the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using their advanced features to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is on filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

**Topics:** Wireshark Display Filters; Writing tcpdump Filters; TCP, UDP, ICMP

---

**DAY 3: Application Protocols and Traffic Analysis**
Day 3 introduces the versatile packet crafting tool Scapy. It 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. The examination of TCP/IP culminates with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols: DNS, HTTP(S), SMTP, and Microsoft communications. Our focus is on protocol analysis, a key skill in intrusion detection. IDS/IPS evasions are the bane of the analyst. We discuss how this enables monitoring and correlating activity and demonstrate with examples.

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

---

**DAY 4: Network Monitoring: Snort and Bro**
The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days of SEC503. Snort and Bro are widely deployed open-source IDS/IPS solutions that have been industry standards for many years. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a look at options and requirements of devices that can sniff and capture the traffic for inspection. Next, the topic of the analyst’s role in the detection process is examined. Before Snort and Bro are discussed, the capabilities and limitations are considered. Snort detection flow, running Snort, and rules are explored with an emphasis on writing efficient rules. It is likely that false positives and negatives will occur and tips for dealing with them are presented. Bro’s unique capability to use its own scripting language to write code to analyze patterns of event-driven behavior is one of the most powerful detection tools available to the analyst. We discuss how this enables monitoring and correlating activity and demonstrate with examples.

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

---

**DAY 5: Network Traffic Forensics**
The penultimate day continues the format of less instruction and more hands-on training using three separate incidents that must be analyzed. The three incident scenarios are introduced with some new material to be used in the related hands-on analysis. This material includes an introduction to network forensics analysis for the first scenario. It continues with using network flow records to assist in analysis of the traffic from the second scenario. It concludes by examining the third scenario, including Command and Control channels and managing analysis when very large packet capture files are involved.

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

---

**DAY 6: NetWars: IDS Version**
The week culminates with a hands-on NetWars: IDS Version challenge. Students compete on teams to answer many questions that require using tools and theory covered in the first five days. This is a great way to end the week because it reinforces what was learned by challenging the student to think analytically and strengthens confidence to employ what was learned in a real-world environment.

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

---

**Who Should Attend**
- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

---

“I got a deeper understanding of the topics from my class. This will help me get more data out of my investigations.”
-Alphonse Wichrowski, Allegiant Air

---

**Online Training**
- **OnDemand**
  - Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**
- Online Training ................................ Jun 10-15
- Online Training ................................ Jul 15-20
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 (CM) 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 day 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 day 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 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.
<table>
<thead>
<tr>
<th>Course Day Descriptions</th>
</tr>
</thead>
</table>
| **DAY 1: Current State Assessment, SOCs, and Security Architecture**  
We begin with the end in mind by defining the key techniques and principles that will allow us to get there. An effective modern Security Operations Center (SOC) 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:** Current State Assessment, SOCs, and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Techniques/Practices |
| **DAY 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. Day 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.  
**Topics:** SOCs/Security Architecture – Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied |
| **DAY 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 days 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.  
**Topics:** Continuous Monitoring Overview, Network Security Monitoring (NSM); Practical NSM Issues; Cornerstone NSM |
| **DAY 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. Day four 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 |
| **DAY 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.  
**Topics:** CSM 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 |
| **DAY 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 week.  
**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  
- Security Operations Center (SOC) analysts, engineers, and managers  
- CND analysts  
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)  

**“SEC511 is a VERY worthwhile addition to the Cyber Defense curriculum for Blue Teamers.”**  
- Robert Peden, NextGear Capital

**Online Training**  
**OnDemand**  
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.  
**vLive**  
Online Training · Simulcast  
Online Training  
- Jun 17-22
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are 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?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o’clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don’t 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 and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come.

Written by a security professional with over 30 years of 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 for the next SANS course in this progression, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to 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 on a high level.”

-Richard Pollich, Broadridge Financial Solutions Inc.
Course Day Descriptions

**DAY 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 day, 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.

**DAY 2: Computer Functions and Networking**
This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using the American Standard Code for Information Interchange (ASCII). We then spend the remainder of the day on networking. All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. The networking discussion begins with a non-technical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You’ll learn about common network hardware such as switches and routers, and terms like “protocol” and “encapsulation.” We’ll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you’ll have a fundamental grasp of any number of critical technical networking acronyms that you’ve often heard but never quite understood, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

**DAY 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, so we will spend some time on it. Not to worry, we won’t take you through the math behind cryptography. Instead, we learn basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a “work factor” in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and “cryptographic hash,” and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?

**DAY 4: Cybersecurity Technologies – Part 1**
Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. We end the day with an examination of several data protection protocols used for email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network (VPN) technologies.

**DAY 5: Cybersecurity Technologies – Part 2**
The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at several security technologies, including compartmentalization, firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), sniffers, content filters, etc. We then take a good look at browser and web security, and the difficulties of securing the web environment. For example, students will 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 day with a look at system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup.

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
- Non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o’clock news
- Professionals with basic computer and technical knowledge in all disciplines 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 cybersecurity and need formal training and certification

“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

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

Simulcast
Online Training .............................. Jul 15-19

Community Events
Cincinnati, OH .............................. Jun 24-28
Tulsa, OK .................................. Aug 12-16
Miami, FL ................................. Aug 12-16

Mentor Events
Daytona Beach, FL ........................ Jun 20 - Aug 8

Private Training
This course is also available through Private Training.
Immeasurable amounts of personal and potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update daily via their devices. Those data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

Many people think using their favorite Internet search engine is sufficient to find the data they need and do not realize that most of the Internet is not indexed by search engines. SEC487 teaches students legitimate and effective ways to find, gather, and analyze these data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the information, we’ll show you how to ensure that it is sound, how to analyze what you’ve gathered, and how to make sure it is useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. You will learn current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base 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.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. More than 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

Author Statement

“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 Author

“Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!”

-Dave Huffman, Rockwell Automation
**Course Day Descriptions**

**DAY 1: Foundations of OSINT**
We begin with the basics and answer the questions "what is OSINT" and "how do people use it." This first day 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 week by learning how to document findings and set up an OSINT platform, and we discuss effective research habits for OSINT analysts. This day 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, making them less useful when delivered to the customer.

**Topics:** Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting Up an OSINT Platform; Effective Research Habits; Creating Sock Puppets

**DAY 2: Gathering, Searching, and Analyzing OSINT**
OSINT data collection begins on day two 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; Creating Your OSINT Process; Harvesting Web Data; OSINT Frameworks; Basic Data: Street Addresses; Basic Data: Phone Numbers; Basic Data: Email Addresses; User Names; Avatars and Reverse Image Searches; Leveraging Search Engines

**DAY 3: Social Media and Geolocation**
Finding data on people, especially basic content such as email addresses, home addresses, and phone numbers, can be made easier using online people search engines. This is how day three kicks off, examining free and paid choices in this data aggregator area 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.

**Topics:** People Searching; Facebook Analysis; LinkedIn Data; Instagram; Twitter Data; Geolocation; Dating and Adult Websites; Web and Traffic Cameras; File Metadata Analysis

**DAY 4: Imagery, Networks, Government, and Business**
Day four focuses on many different but related OSINT issues. We begin by looking at how various mapping sites can assist our assessments with aerial data, distance-measuring, and "street view" imagery. Moving beyond using just one vendor’s mapping system, students will work with a variety of free, online mapping resources.

**Topics:** Remote Location Recon; IP Address and Whois; IP Address Geolocation; Domain Name System (DNS); Wireless Networks; Recon Tool Suites and Frameworks; U.S. Government Data; Researching Companies

**DAY 5: The Dark Web and International Issues**
The entire morning of day five focuses on understanding and using three of the most popular dark web networks for OSINT purposes. 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. The first module in the afternoon examines how blue teams (cyber defenders) can use monitoring to receive alerts when data of interest appear on the Internet. We then shift our focus to data found on "paste” sites. These websites sometimes contain content such as user names and passwords of compromised user accounts, detailed network information about our target’s systems, or just data that our customers need to know.

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

**DAY 6: Capstone: Capture (and Present) the Flag**
The capstone for the course is a group event that brings together everything that students learned throughout the week. This is not a “canned” Capture the Flag (CTF) 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 a certain group of people. The output from this work will be turned in as a “deliverable” to the “client” (the instructor), and then the three teams with the most-complete work will present their research to the class for voting. This multi-hour, hands-on event will reinforce what the students practiced in the Solo CTF the day before and add the complexity of performing OSINT assessments under pressure and in a group.

**Online Training**

- **OnDemand**
  Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

- **vLive**
  Online Training ......................... Jun 11 - Jul 18

---

**Community Events**

- **Ottawa, ON**  Sept 16-21

---

27
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.

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 is a very valuable course to a Network/Security Administrator. The first chapter of Defensible Network Architecture is worth the price of admission in of itself.”

-Ryan Bast, Subzero Group, Inc.

---


**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

**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 Training**

<table>
<thead>
<tr>
<th>Training Event</th>
<th>Location</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANSFIRE</td>
<td>Washington, DC</td>
<td>Jun 17-22</td>
</tr>
<tr>
<td>Virgin Beach</td>
<td>Virginia Beach, VA</td>
<td>Aug 19-24</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 9-14</td>
</tr>
<tr>
<td>San Francisco Fall</td>
<td>San Francisco, CA</td>
<td>Sep 23-28</td>
</tr>
<tr>
<td>CDI</td>
<td>Washington, DC</td>
<td>Dec 14-19</td>
</tr>
</tbody>
</table>

**Summit Events**

- Supply Chain Cybersecurity, Arlington, VA: Aug 14-19
- Purple Team, Las Colinas, TX: Oct 23-28

**Community Events**

- New York, NY: Jul 29 - Aug 3

**Private Training**

This course is also available through Private Training.

---

**SEC501 is available via (subject to change):**

- 6 Day Program
- 38 CPEs
- Laptop Required
DAY 1: Defensive Network Architecture
This course day 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.
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

DAY 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. On day two, 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

DAY 3: Network Detection and Packet Analysis
“Prevention is ideal, but detection is a must” is a critical motto for network security professionals. While organizations always want to prevent as many attacks as possible, some adversaries will still sneak into the network. In cases where an attack is not successfully prevented, network security professionals need to analyze network traffic to discover attacks in progress, ideally stopping them before significant damage is done. Packet analysis and intrusion detection are at the core of such timely detection. Organizations need to not only detect attacks but also to react in a way that ensures those attacks can be prevented in the future.
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

DAY 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 into 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.
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

DAY 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 tripping 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.

DAY 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.

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
Simulcast
Online Training ...................................... Jun 17-22
Online Training ...................................... Jul 22-27
Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn how to use PowerShell to automate Windows security management across an Active Directory enterprise. You won’t just learn PowerShell syntax, you’ll learn how to leverage PowerShell as a platform for security.

You’ve run a vulnerability scanner and applied patches – now what? A major theme of this course is defensible architecture: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we’ll never win, and we’ll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT’S TOO LATE. We need to prevent pass-the-hash attacks and Kerberos Golden Ticket attacks as much as possible, not just detect them.

Perhaps you’ve taken a hacking course at SANS and now you want to learn more Windows and Active Directory attack mitigations: SEC505 is that course.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don’t have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. Many of the PowerShell scripts written by the course author are free in GitHub (go to http://SEC505.com).

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn’t just good for security, it can save money too.

SEC505 is designed for the blue team to block the attacks of the red team.

The focus of this course is on how to automate the NSA Top 10 Mitigations, the CIS Critical Security Controls related to Windows, and the MITRE ATT&CK mitigations for Windows, especially the ones that are the most difficult to implement in large environments.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to prove your Windows security expertise. The GCWN certification counts towards a Master’s Degree in Information Security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8140 computing environment requirement. The GCWN is also a foundational certification for soldiers in the U.S. Army’s 255-S Information Protection Program. For DoD students, we will see how to apply the NSA/DISA Secure Host Baseline.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don’t cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and Windows security at the same time!
Course Day Descriptions

**DAY 1: Learn PowerShell Scripting**
This course section covers what you need to know to get started using PowerShell. You don’t need to have any prior scripting or programming experience. We have PowerShell labs throughout the week, so today is not the only PowerShell material. We start with the essentials, then go more in depth as the week progresses. Don’t worry, you won’t be left behind, the PowerShell labs walk you through every step.

**Topics:** Why Is PowerShell So Important and Dangerous?; Writing Your Own Scripts, Functions, and Modules; PowerShell Remoting; Getting Up and Running Quickly with PowerShell

**DAY 2: Host Hardening and Active Directory Scripting**
Running a vulnerability scanner is easy, but remediating vulnerabilities in a large enterprise is hard. Most vulnerabilities are fixed by applying patches, but this course does not talk about patch management, you’re doing that already. What about the other vulnerabilities, the ones not fixed by applying patches? These vulnerabilities are, by definition, remediated by configuration changes. That’s the hard part. We need a secure architecture designed for SecOps/DevOps.

**Topics:** Continuous Secure Configuration Enforcement; Remote PowerShell Script Execution with Group Policy; Server Hardening Automation; PowerShell for Active Directory

**DAY 3: Smart Tokens and Public Key Infrastructure (PKI)**
Running a Public Key Infrastructure (PKI) is pretty much mandatory for Microsoft security and cloud computing today. The best form of multi-factor authentication (MFA) is a USB smart token integrated into Active Directory. We need digital certificates for SSL/TLS, wireless authentication, VPN gateways, code signing, and much more. This day of the course is basically one long hands-on lab to install and configure a full Windows Server PKI. This includes a root Certification Authority (CA), Group Policy certificate auto-enrollment on endpoints, Online Certificate Status Protocol (OCSP) revocation checking, private key roaming for users, smart card/token certificate deployment, and, of course, lots of PowerShell examples.

**Topics:** Why Is a PKI Necessary?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

**DAY 4: Protecting Admin Credentials and PowerShell JEA**
Why do submarines have pressure doors to seal off compartments? Because they are designed to assume a breach will occur. In a Windows environment, a security breach will occur, so we must design the architecture with an “assume breach” mindset as well. If we assume that some day the computers and credentials of our administrators will be compromised, then how do we build damage control into the network from the beginning? This is not about detection and incident response. The challenge here is how to design for damage control when we delegate administrative privileges. We need to proactively design damage control into the architecture, not wait until after there is a breach (when it’s too late).

**Topics:** Restricting Unnecessary Admin Privileges; Compromise of Administrative Powers; PowerShell Just Enough Admin (JEA); Active Directory Permissions and Delegation

**DAY 5: Thwarting Hackers Inside the Network**
You are already applying patches and updating anti-virus signatures. But endpoint protection is much more than that. Because most advanced malware infections start with a compromised endpoint, we want to proactively build defensibility and damage control into our systems using a “zero trust” or “assume breach” model. How? AppLocker is an application whitelisting tool built into Windows to control which executables, scripts, DLLs and installer packages users may run. If hackers or malware attempt to launch an unauthorized process post-exploitation, the aim is to block it and log it. In the lab, we’ll use PowerShell and Group Policy to manage AppLocker. Application whitelisting can be hard to manage if used too aggressively, so we’ll also talk about how to get started without making the help desk phone ring off the hook.

**Topics:** Anti-Exploitation, TCP/UDP Port Permissions for Role-Based Access Control, Windows Defender Firewall

**DAY 6: Blue Team PowerShell: WMI, DNS, RDP, and SMB**
Hackers love the Windows Management Instrumentation (WMI) service, and so should we. We are the linebackers on the Blue Team and the WMI service was made to benefit us, not hackers. The WMI service is enabled by default and accessible over the network. Through WMI we can do remote command execution (without PowerShell being installed at the target), forcibly log off the user, reboot the machine, stop services, search for processes running as Administrator, kill any process, and much more. The WMI service is nearly all-powerful and it’s built for remote administration. PowerShell is tightly integrated into WMI, and we’ll look at several PowerShell examples.

**Topics:** PowerShell and WMI; Hardening DNS, Dangerous Protocols We Can’t Live Without

**Who Should Attend**
- Security Operations personnel
- Blue Team players who were terrified by SEC504
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the NSA/DoD Secure Host Baseline
- Individuals deploying or managing a PKI or smart cards
- Anyone wanting a more rugged Windows architecture

“This class provided real-world examples and sample scripts to make a Windows-centric environment fundamentally more secure.”

-Nick Boardman, HRSD

**Online Training**
**OnDemand**
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**
Online Training ......................... Jun 17-22
This course provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix.

The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS’s practical approach uses hands-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

### Topics

- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a Centralized Logging Infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server Lockdown for Linux and Unix
- Controlling Root Access with sudo
- SELinux and chroot() for Application Security
- DNSSEC Deployment and Automation
- mod_security and Web Application Firewalls
- Secure Configuration of BIND, Sendmail, and Apache
- Forensic Investigation of Linux Systems

### Author Statement

“A wise man once said, ‘How are you going to learn anything if you know everything already?’ And yet there seems to be a quiet arrogance in the Unix community that we have figured out all of our security problems, as if to say, ‘Been there, done that.’ All I can say is that what keeps me going in the Unix field, and the security industry in particular, is that there is always something new to learn, discover, or invent. In 20 plus years on the job, what I have learned is how much more there is that I can learn. I think this is also true for the students in my courses. I regularly get comments back from students who say things like, ‘I have been using Unix for 20 years, and I still learned a lot in this class.’ That is really rewarding.”

–Hal Pomeranz

“Linux security courses are a rare commodity and a valuable resource to the security professional.”

–Trevor Sellers, IDA Center for Communications Research
**Who Should Attend**

- Security professionals looking to learn the basics of securing Unix operating systems
- Experienced administrators looking for in-depth descriptions of attacks on Unix systems and how they can be prevented
- Administrators needing information on how to secure common Internet applications on the Unix platform
- Auditors, incident responders, and InfoSec analysts who need greater insight into Linux and Unix security tools, procedures, and best practices

“**This course gave me a better understanding of Linux internals and specific threat hunting ideas that I will use in my environment.**”

- Shelby Peterson, Adobe
SEC530: Defensible Security Architecture and Engineering

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.

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.

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.

Hands-on labs 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.

You Will Learn To

- Layer security solutions ranging from network to endpoint and cloud-based technologies
- Understand the implications of proper placement of technical controls
- Tune, adjust, and implement security techniques, technologies, and capabilities
- Think outside the box on using common security solutions in innovative ways
- Balance detection with prevention while allowing for better response times and capabilities
- Understand where prevention technologies are likely to fail and how to supplement them with specific detection technologies
- Understand how security infrastructure and solutions work at a technical level and how to better implement them

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

“There are no other courses out there that cover practical hands-on security architecture.”

- Chris Kuhl, Premier Health
Course Day Descriptions

**DAY 1: Defensible Security Architecture and Engineering**
This first section of the course describes hardening systems and networks at every layer, from layer one (physical) to layer seven (applications and data). To quote Richard Bejtlich’s *The Tao of Network Security Monitoring*, defensible networks “encourage, rather than frustrate, digital self-defense.”

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

---

**DAY 2: Network Security Architecture and Engineering**
Day 2 continues hardening the infrastructure and moves on to layer three: routing. 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% of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. This section 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 of VPN and stateful layer three/four firewalls.

**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

---

**DAY 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.

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

---

**DAY 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.

**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

---

**DAY 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.

**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

---

**DAY 6: Hands-On Secure-the-Flag Challenge**
The course culminates in a team-based Design-and-Secure-the-Flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. 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

“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
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 day one and all of day 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 day 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.

“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.
Cloud Forensics

Pen Testing; Intrusion Detection in the Cloud; Cloud IR and Event Management; Threats to Cloud Computing; Vulnerability Management in the Cloud; Cloud so we need to focus on automation and event-driven defenses more than ever.

Our final topics on day four include incident response and forensics (also topics professionals need to know what their best options are and how to get this done. is an area that has definitely changed from what we’re used to in-house, so security how to monitor and automate our processes to better carry out this detection. This defensive side, we start with network-based and host-based intrusion detection, and then turn our attention toward SecDevOps 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 we can develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from day four, 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 class with a few more tools and tactics, followed by a sampling of real-world use cases.

Topics: Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability

DAY 1: Cloud Security Foundations

The first day of the course starts out with an introduction to the cloud, including terminology, taxonomy, and basic technical premises. We also examine what is happening in the cloud today, and cover the spectrum of controls and strategies, including the Cloud Security Alliance, including the Cloud Controls Matrix, the 14 major themes of cloud security, and other research available. Next we spend time on cloud policy and planning, delving into the changes an organization needs to make for security and IT policy to properly embrace the cloud. After all the legwork is done, we’ll start talking about some of the main technical considerations for the different cloud models. We’ll start by breaking down Software-as-a-Service (SaaS) and some of the main types of security controls available. A specialized type of Security-as-a-Service (SecaaS) known as Cloud Access Security Brokers (CASBs) will also be explained, with examples of what to look for in such a service. We’ll wrap up with an introduction to Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) controls, which will set the stage for the rest of the course.

Topics: Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; Cloud Policy and Planning; SaaS Security; Cloud Access Security Brokers; Intro to PaaS and IaaS Security Controls

DAY 2: Core Security Controls for Cloud Computing

The second day of SEC545 compares traditional in-house controls with those in the cloud today. Some controls are similar and mostly compatible, but not all of them. Since most cloud environments are built on virtualization technology, we walk through a short virtualization security primer, which can help teams building hybrid clouds that integrate with internal virtualized assets, and also help teams properly evaluate the controls cloud providers offer in this area. We’ll then break down cloud network security controls and tradeoffs, since this is the area that is very different from what we’ve traditionally run in-house. For PaaS and IaaS environments, it’s critical to secure virtual machines (instances) and the images we deploy them from, so we cover this next. At a high level, we’ll also touch on identity and access management for cloud environments to help control and monitor who is accessing the cloud infrastructure, as well as what they’re doing there. We also cover data security controls and types, including encryption, tokenization, and more. Specific things to look for in application security are laid out as the final category of overall controls. We then pull it all together to demonstrate how you can properly evaluate a cloud provider’s controls and security posture.


DAY 3: Cloud Security Architecture and Design

Instead of focusing on individual layers of our cloud stack, we start day three by building the core security components. We’ll break down cloud security architecture best practices and principles that most high-performing teams prioritize when building or adding cloud security controls and processes to their environments. We start with infrastructure and core component security – in other words, we need to look at properly locking down all the pieces and parts we covered on day two! This then leads to a focus on major areas of architecture and security design. The first is building various models of access control and compartmentalization. This involves breaking things down into two categories: identity and access management (IAM) and network security. We delve into these in significant depth, as they can form the backbone of a sound cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with 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 disaster recovery and continuity, and so this is covered as well.

Topics: Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability

DAY 4: Cloud Security – Offense and Defense

There are many threats to our cloud assets, so the fourth day of the course begins with an in-depth breakdown of the types of threats out there. We’ll look at numerous examples. The class also shows students 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. Scanning and pen testing the cloud used to be challenging due to restrictions put in place by the cloud providers themselves. But today it is easier than ever. There are some important points to consider when planning a vulnerability management strategy in the cloud, and this class touches on how to best scan your cloud assets and which tools are available to get the job done. Pen testing naturally follows this discussion, and we talk about how to work with the cloud providers to coordinate tests, as well as how to perform testing yourself. 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. Our final topics on day four include 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.

Topics: Threats to Cloud Computing, Vulnerability Management in the Cloud, Cloud Pen Testing; Intrusion Detection in the Cloud; Cloud IR and Event Management, Cloud Forensics

DAY 5: Cloud Security Automation and Orchestration

On our final day, 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 toward SecDevOps 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 we can develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from day four, 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 class with a few more tools and tactics, followed by a sampling of real-world use cases.

Topics: Scripting and Automation in the Cloud; SecDevOps Principles; Creating Secure Cloud Workflows; Building Automated Event Management; Building Automated Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up

Community Events

Raleigh, NC ................................. Jun 3-7
Toronto, ON .................................. Jun 10-14
Sterling, VA ................................. Jul 8-12
Anaheim, CA ................................. Jul 22-26
Kansas City, KS ............................ Jul 29 - Aug 2

Online Training

OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
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

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. This 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.
DAY 1: SIEM Architecture and SOF-ELK
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 handle 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. Day one is designed to get them up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK 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

DAY 2: Service Profiling with SIEM
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 will be 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 they are 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

DAY 3: Advanced Endpoint Analytics
The value in endpoint logs provides tremendous visibility in detecting attacks. In particular, with regard to finding post-compromise activity, endpoint logs can quickly become second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousands of events per day. Multiply this by the number of systems in your environment and it is no surprise that 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. Workstation 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

DAY 4: Baselining and User Behavior Monitoring
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 or 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

DAY 5: Tactical SIEM Detection and Post-Mortem Analysis
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, preventing compromise is the beginning, not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires—and if a single one is tripped, we can quickly detect it 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

DAY 6: Capstone: Design, Detect, Defend
The course culminates in a team-based Design, Detect, and Defend-the-Flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From building a logging architecture to augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to find 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

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

Simulcast
Online Training
Jun 17-22
Online Training
Aug 12-17

Mentor Events
- Lessburg, VA
  Jul 16 - Sep 3

Private Training
This course is also available through Private Training.
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 gives really good background about adversary behavior and the steps needed to detect it.”

-Tarot Wake, Halkyn Consulting Ltd
DAY 1: Introduction and 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 one exercises.

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

DAY 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

DAY 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

DAY 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, Kerberos, 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?

DAY 5: Action on Objectives, Threat Hunting, and Incident Response
Section five 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 DCSync
- 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 day.

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

DAY 6: APT Defender Capstone
The course culminates in a team-based Defend-the-Flag competition. Section six 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 cyber security controls promoted all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge. Note that OnDemand students will enjoy this exercise on an individual basis. As always, SANS SME’s are available to support every OnDemand student’s experience.

Topics: Applying Previously Covered Security Controls In-depth; Reconnaissance; Weaponization; Delivery; Exploitation; Installation; Command and Control; Action on Objectives
SEC560: Network Penetration Testing and Ethical Hacking

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, and web app manipulation, 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 web apps, pivoting through the target environment to model the attacks of real-world bad guys 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

Live Training

<table>
<thead>
<tr>
<th>City</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kansas City</td>
<td>Kansas City, MO</td>
<td>Jun 10-15</td>
</tr>
<tr>
<td>SANSFIRE</td>
<td>Washington, DC</td>
<td>Jun 17-22</td>
</tr>
<tr>
<td>Charlotte</td>
<td>Charlotte, NC</td>
<td>Jul 8-13</td>
</tr>
<tr>
<td>Pittsburgh</td>
<td>Pittsburgh, PA</td>
<td>Jul 8-13</td>
</tr>
<tr>
<td>Rocky Mountain</td>
<td>Denver, CO</td>
<td>Jul 15-20</td>
</tr>
<tr>
<td>Crystal City</td>
<td>Arlington, VA</td>
<td>Aug 5-10</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Aug 12-17</td>
</tr>
<tr>
<td>Virginia Beach</td>
<td>Virginia Beach, VA</td>
<td>Aug 19-24</td>
</tr>
<tr>
<td>Tampa-Clearwater</td>
<td>Clearwater, FL</td>
<td>Aug 25-30</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 9-14</td>
</tr>
<tr>
<td>Raleigh</td>
<td>Raleigh, NC</td>
<td>Sep 16-21</td>
</tr>
<tr>
<td>San Francisco</td>
<td>San Francisco, CA</td>
<td>Sep 23-28</td>
</tr>
<tr>
<td>N. VA Fall</td>
<td>Reston, VA</td>
<td>Sep 30 - Oct 5</td>
</tr>
<tr>
<td>Baltimore Fall</td>
<td>Baltimore, MD</td>
<td>Oct 7-12</td>
</tr>
<tr>
<td>Seattle Fall</td>
<td>Seattle, WA</td>
<td>Oct 14-19</td>
</tr>
<tr>
<td>Denver</td>
<td>Denver, CO</td>
<td>Oct 14-19</td>
</tr>
<tr>
<td>CIDI</td>
<td>Washington, DC</td>
<td>Dec 14-19</td>
</tr>
</tbody>
</table>

Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Defense</td>
<td>Redondo Beach, CA</td>
<td>Jun 5-10</td>
</tr>
<tr>
<td>Oil &amp; Gas Cybersecurity</td>
<td>Houston, TX</td>
<td>Sep 17-22</td>
</tr>
<tr>
<td>Pen Test HackFest</td>
<td>Bethesda, MD</td>
<td>Nov 20-25</td>
</tr>
</tbody>
</table>
**Course Day Descriptions**

**DAY 1: Comprehensive Pen Test Planning, Scoping, and Recon**
In this section of the course, you will develop the skills needed to conduct a best-of-breed, high-value penetration test. We will go in-depth on how to build 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 will 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 document metadata analysis to pull sensitive information about a target environment, as well as a lab using Recon-ng to plunder a target’s DNS infrastructure for information such as the anti-virus tools the organization relies on.

**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; Effective Pen Test Reporting to Maximize Impact; Mining Search Engine Results; Document Metadata Extraction and Analysis

**DAY 3: Exploitation**
In this 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. We’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/Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis; Hands-On; Implementing Port Forwarding for Merciless Pivots; How to Leverage PowerShell Empire to Plunder a Target Environment

**DAY 5: In-Depth Password Attacks and Web App Pen Testing**
In this section of the course, we’ll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You’ll custom-compile John the Ripper to optimize its performance in cracking passwords. You’ll look at the amazingly full-featured Cain tool, running it to crack sniffed Windows authentication messages. We’ll see how Rainbow Tables really work to make password cracking much more efficient, all hands-on. And we’ll cover powerful “pass-the-hash” attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app attack techniques with hands-on labs for every topic we address. We’ll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

**Topics:** Password Cracking with John the Ripper; Sniffing and Cracking Windows Authentication Exchanges Using Cain; Using Rainbow Tables to Maximize Effectiveness; Pass-the-Hash Attacks with Metasploit and More; Finding and Exploiting Cross-Site Scripting; Utilizing Cross-Site Request Forgery Flaws; Data Plundering with SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

**DAY 2: In-Depth Scanning**
We next focus on the vital task of mapping the target environment’s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We will 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 will also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the day covering the latest scanning techniques and the incredible WMIC toolset to access and pivot through a target organization. We’ll then turn our attention to password guess attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines using the great Mimikatz Kiwi tool. Finally, we’ll look at Metasploit’s fantastic features for pivoting, including the msfconsole route command.

**Topics:** Windows Command Line Kung Fu for Penetration Testers; PowerShell’s Amazing Post-Exploitation Capabilities; Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi

**DAY 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

---

**Community Events**
- Falls Church, VA .......................... Jun 24-29
- Mentor Events
  - San Antonio, TX .......................... Oct 1 - Nov 19

**Private Training**
This course is also available through Private Training.

**Online Training**
- OnDemand
  - Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**
- Online Training ......................... Jul 8-13
- Online Training ......................... Sep 9-14

43
SEC542: Web App Penetration Testing and Ethical Hacking

You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- 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
- 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 Burp Suite 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 a complete web penetration test during the Capture-the-Flag exercise to bring techniques and tools together into a comprehensive test

Web applications play a vital role in every modern organization. However, if your organization doesn’t 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, and 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, and 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 impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to 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. This course will help you demonstrate the true impact of web application flaws through exploitation.

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 having 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 day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers 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.
Course Day Descriptions

DAY 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 will also examine different authentication systems, including Basic, Digest, Forms and Windows integrated authentication, and discuss how servers use them and attackers abuse them.

Topics: Overview of the Web from a Penetration Tester’s Perspective; Exploring the Various Servers and Clients; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; WHOIS and DNS Reconnaissance; The HTTP Protocol; WebSocket; Secure Sockets Layer (SSL) Configurations and Weaknesses; Heartbleed Exploitation; Utilizing the Burp Suite in Web App Penetration Testing

DAY 2: Configuration, Identity, and Authentication Testing
The second day starts the actual penetration testing process, beginning with the reconnaissance and mapping phases. Reconnaissance includes gathering publicly available information regarding the target application and organization, identifying the machines that support our target application, and building a profile of each server, including the operating system, specific software and configuration. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

Topics: Scanning with Nmap; Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Exploring Virtual Hosting and its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Learning Tools to Spider a Website; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock; Web Authentication; Username Harvesting and Password Guessing; Fuzzing; Burp Intruder

DAY 3: Injection
This section continues to explore our methodology with the discovery phase. We will build on the information started the previous day, exploring methods to find and verify vulnerabilities within the application. Students will also begin to explore the interactions between the various vulnerabilities.

Topics: Session Tracking; Authentication Bypass Flaws; Mutillidae; Command Injection; Directory Traversal; Local File Inclusion (LFI); Remote File Inclusion (RFI); SQL Injection; Blind SQL Injection; Error-Based SQL Injection; Exploiting SQL Injection; SQL Injection Tools; sqlmap

DAY 4: XXE and XSS
On day four, students continue exploring the discovery phase of the methodology. We cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF/XSRF). Manual discovery methods are employed during hands-on labs.

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

DAY 5: CSRF, Logic Flaws, and Advanced Tools
On the fifth day, we launch actual exploits against real-world applications, building on the previous three steps, 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 the four-step attack methodology.

Topics: Cross-Site Request Forgery (CSRF), Python for Web App Penetration Testing; WPScan; w3af; Metasploit for Web Penetration Testers; Leveraging Attacks to Gain Access to the System; How to Pivot: Our Attacks Through a Web Application; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities; When Tools Fail

DAY 6: Capture the Flag
On day six, 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.

Who Should Attend
- General security Practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website developers and architects

Private Training
This course is also available through Private Training.

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform

VLive
Online Training ............................. Jul 9 - Aug 15
Simulcast
Online Training ............................. Jul 15-20
Online Training ............................. Sep 9-14

45
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

SEC460: Enterprise Threat and Vulnerability Assessment

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 days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day 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 Is available via (subject to change):

Live Training

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Program Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 17-22</td>
<td>Washington, DC</td>
<td>NEW</td>
</tr>
<tr>
<td>Jul 15-20</td>
<td>Denver, CO</td>
<td></td>
</tr>
<tr>
<td>Jul 22-27</td>
<td>San Francisco, CA</td>
<td></td>
</tr>
<tr>
<td>Aug 25-30</td>
<td>Clearwater, FL</td>
<td></td>
</tr>
<tr>
<td>Sep 9-14</td>
<td>Las Vegas, NV</td>
<td></td>
</tr>
<tr>
<td>Oct 14-19</td>
<td>Denver, CO</td>
<td></td>
</tr>
<tr>
<td>Dec 14-19</td>
<td>Washington, DC</td>
<td></td>
</tr>
<tr>
<td>Jun 5-10</td>
<td>Redondo Beach, CA</td>
<td>Summit Events</td>
</tr>
<tr>
<td>Nov 20-25</td>
<td>Bethesda, MD</td>
<td></td>
</tr>
</tbody>
</table>

Network Security

Rocky Mountain
San Francisco Summer
Tampa-Clearwater

CDI

Summit Events

Enterprise Defense
Pen Test HackFest
Course Day Descriptions

DAY 1: Methodology, Planning, and Threat Modeling
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 Modeling; Generating Compounding Interest from Threat Intelligence and Avoiding Information Overload; The Vulnerability Assessment Framework; Overview of Comprehensive Network Scanning; Compliance Standards and Information Security; Team Operations and Collaboration

DAY 2: Discovery
Having mastered the structural foundations of vulnerability management, we 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: Active and Passive Reconnaissance; 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; Introduction to PowerShell

DAY 3: Enhanced Vulnerability Scanning and Automation
We begin day three 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 and gaining 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.


DAY 4: Vulnerability Validation, Triage, and Data Management
Over the course of this day 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 for analyzing vulnerability data across an organization. Later in the day, 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

DAY 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.


DAY 6: Vulnerability Assessment Foundry 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 module 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 unique systems, including Web Applications; Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk
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.

Or, 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.

You Will Be Able To
- Modify existing open-source tools to customize them 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

SEC573 is available via (subject to change):

Live Training

<table>
<thead>
<tr>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANSFIRE</td>
<td>Washington, DC</td>
</tr>
<tr>
<td>Columbia</td>
<td>Columbia, MD</td>
</tr>
<tr>
<td>Virginia Beach</td>
<td>Virginia Beach, VA</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
</tr>
</tbody>
</table>

Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFIR</td>
<td>Austin, TX</td>
<td>Jul 27 - Aug 1</td>
</tr>
<tr>
<td>THIR</td>
<td>New Orleans, LA</td>
<td>Oct 2-7</td>
</tr>
<tr>
<td>Pen Test HackFest</td>
<td>Bethesda, MD</td>
<td>Nov 20-25</td>
</tr>
</tbody>
</table>

Private Training

This course is also available through Private Training.
**Course Day Descriptions**

**DAY 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

**DAY 2: Essentials Workshop with MORE pyWars**
You will never learn to program by staring at PowerPoint slides. The second day continues the hands-on, lab-centric approach established on day one. 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; argparse Module

**DAY 3: Defensive Python**
In this 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. Forensicos and offensive security professional 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

**DAY 4: Forensics Python**
On day four we will play the role of a forensics 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 these skills covered on day four 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

**DAY 5: Offensive Python**
On day five we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for incident response or systems administration, but our focus will be on offensive operations.

**Topics:** Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Using the Select Module for Asynchronous Operations; Python Objects; Argument Packing and Unpacking

**DAY 6: Capture the Flag**
In this final section, you will be placed on a team with other students. You will 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!

"SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs."

-Caleb Jaren, Microsoft

**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

**You Will Receive**
- A USB containing a virtual machine filled with sample code and working examples
- A copy of The Python Pocket Reference published by O’Reilly Press
- MP3 audio files of the complete course lecture

**Online Training**
- **OnDemand**
  Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

- **Simulcast**
  Online Training .............................. Sep 9-14
Imagine an attack surface that is spread across your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. Such a surface already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

SEC575 is designed to give you the skills you need to understand the security strengths and weaknesses in 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 throughout 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 how to 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, or better informed on 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 having 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.
## Course Day Descriptions

### DAY 1: Device Architecture and Common Mobile Threats

The first module of SEC575 quickly 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 Pie), Apple iOS 12, and the Apple Watch and Google Wear platforms. 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. We will examine the tools used to evaluate mobile devices as part of establishing a lab environment for mobile device assessments, including the analysis of mobile malware affecting Android and non-jailbroken iOS devices. Finally, we will address the threats of lost and stolen devices (and opportunities for a pen tester), including techniques to bypass mobile device lock screens.

**Topics:** Mobile Problems and Opportunities; Mobile Device Platform Analysis; Wearable Platforms; Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

### DAY 2: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and on the evaluation of mobile applications. This module is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts. We will also start to evaluate the security of mobile applications, using network capture analysis tools to identify weak network protocol use and sensitive data disclosure over the network. Finally, we’ll wrap up the module with an introduction to reverse engineering of iOS and Android applications using decompilers, disassemblers, and by manual analysis techniques.

**Topics:** Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and File System Architecture; Network Activity Monitoring; Static Application Analysis

### DAY 3: Mobile Application Reverse Engineering

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. Through lecture and hands-on exercises in this module, with some analysis skills, you will be able to evaluate critical mobile applications to determine the type of access threats and information disclosure threats they represent. In this module we will use automated and manual application assessment tools to evaluate iOS and Android apps. We’ll build upon the static application analysis skills covered in Module 2 to manipulate application components, including Android Intents and iOS URL extensions. We’ll also learn and practice techniques for manipulating iOS and Android applications, such as method swizzling on iOS, and disassembly, modification, and reassembly of Android apps. The module ends with a look at a consistent system for evaluating and grading the security of mobile applications using the Application Report Card Project.

**Topics:** Automated Application Analysis Systems; Reverse Engineering Obfuscated Applications; Application Report Cards

### DAY 4: Penetration Testing Mobile Devices – Part 1

An essential component of developing a secure mobile device deployment is to perform or outsource a penetration test. Through ethical hacking and penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. 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 your organization identify and resolve vulnerabilities before they become incidents.

**Topics:** Manipulating Application Behavior; Using Mobile Device Remote Access Trojans; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks

### DAY 5: Penetration Testing Mobile Devices – Part 2

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation. Hands-on exercises are used throughout the module to practice these attacks, exploiting both vulnerable mobile applications and the supporting back-end servers.

**Topics:** Network Manipulation Attacks; Sidejacking Attacks; SSL/TLS Attacks; Client-Side Injection Attacks; Web Framework Attacks; Back-end Application Support Attacks

### DAY 6: Capture-the-Flag Event

In the final module of SEC575 we will pull together all the concepts and technology covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles, including designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. 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.

---

**Simulcast**

| Online Training | Aug 12-17 |

**vLive**

| Online Training | Oct 22 - Dec 5 |

“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
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 skills are “must-haves” for any high-performing security organization.

For many analysts, “wireless” was once synonymous with “WiFi,” 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 WiFi 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 skill set 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 WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi 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 WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device’s security for use within your organization. Beyond analyzing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.
<table>
<thead>
<tr>
<th>Course Day Descriptions</th>
</tr>
</thead>
</table>
| **DAY 1: WiFi Data Collection and Analysis**  
The first section of the course quickly looks at wireless threats and attack surfaces and analyzes where you will likely see non-WiFi systems deployed in modern networks. We start off with a look at fundamental analysis techniques for evaluating WiFi networks, including the identification and analysis of rogue devices, and finish with a dive into remote penetration testing techniques using compromised Windows 10 and macOS devices to pivot.  
**Topics:** Characterize the Wireless Threat; Sniffing WiFi; Rogue Access Point (AP) Analysis |
| **DAY 2: WiFi Attack and Exploitation Techniques**  
After developing skills needed to capture and evaluate WiFi activity, we start our look at exploiting WiFi, targeting AP and client devices. We cover techniques that apply to any WiFi products, from consumer to enterprise-class devices, focusing on understanding protocol-level deficiencies that will continue to be applied throughout the course on non-WiFi wireless systems as well.  
**Topics:** Exploiting WiFi Hotspots; WiFi Client Attacks; Exploiting WEP; Denial of Service (DoS) Attacks; WiFi Fuzzing for Bug Discovery |
| **DAY 3: Enterprise WiFi, DECT, and ZigBee Attacks**  
We finish our look at WiFi attack techniques with a detailed look at assessing and exploiting WPA2 networks. Starting with WPA2 consumer networks, we investigate the flaws associated with pre-shared key networks and WiFi Protected Setup (WPS) deployments, continuing with a look at exploiting WPA2 Enterprise networks using various Extensible Authentication Protocol (EAP) methods. We continue to investigate the security of wireless networks on day 3, switching to non-WiFi analysis with a look at exploiting the worldwide Digital Enhanced Cordless Telephony (DECT) standard to capture and export audio conversations from cordless headsets and phones. We also investigate the security of ZigBee and IEEE 802.15.4 networks, looking at cryptographic flaws, key management failures, and hardware attacks.  
**Topics:** Attacking WPA2 Pre-Shared Key Networks; Attacking WPA2 Enterprise Networks; Attacking Digital Enhanced Cordless Telephony Deployments; Attacking ZigBee Deployments |
| **DAY 4: Bluetooth and Software-Defined Radio Attacks**  
Bluetooth technology is nearly as pervasive as WiFi, with widespread adoption in smart phones, fitness trackers, wireless keyboard, smart watches, and more. In this module, we dig into the Bluetooth Classic, Enhanced Data Rate, and Low Energy protocols, including tools and techniques to evaluate target devices for vulnerabilities. Immediately following our look at Bluetooth technology, we jump into the practical application of Software-Defined Radio (SDR) technology to identify, decode, and assess proprietary wireless systems. We investigate the hardware and software available for SDR systems, and look at the tools and techniques to start exploring this exciting area of wireless security assessment.  
**Topics:** Bluetooth Introduction and Attack Techniques; Bluetooth Low Energy Introduction and Attack Techniques; Practical Application of Software-Defined Radio (SDR) |
| **DAY 5: RFID, Smart Cards, and NFC Hacking**  
On day 5, we evaluate RFID technology in its multiple forms to identify the risks associated with privacy loss and tracking, while also building an understanding of both low-frequency and high-frequency RFID systems and NFC. We examine the security associated with contactless Point of Sale (PoS) terminals, including Apple Pay and Google Wallet, and proximity lock access systems from HID and other vendors. We also examine generalized techniques for attacking smart card systems, including critical data analysis skills needed to bypass the intended security of smart card systems used for mass transit systems, concert venues, bike rentals, and more.  
**Topics:** RFID Overview; RFID Tracking and Privacy Attacks; Low-Frequency RFID Attacks; Exploiting Contactless RFID Smart Cards; Attacking NFC |
| **DAY 6: Capture-the-Flag Event**  
On the last day of class, we will pull together all the concepts and technology we have covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles: identifying unauthorized/rogue WiFi access points, attacking live and recorded WiFi networks, decoding proprietary wireless signals, exploiting smart card deficiencies, and more. During this wireless 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**

- 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

---

“SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks.”

-Garret Picchioni, Salesforce
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, with 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 day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

This course offers 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 the 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

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 WebSockets
- 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

SEC642 is available via (subject to change):

**Live Training**

- **SANSFIRE** .............. Washington, DC ........ Jun 17-22
- San Jose .................. San Jose, CA ............. Aug 12-17
- **Network Security** ..... Las Vegas, NV ........ Sep 9-14

**Summit Events**

- Pen Test HackFest ........ Bethesda, MD ........ Nov 20-25

**Private Training**

This course is also available through Private Training.

**Online Training**

**OnDemand**

Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**

Online Training .................................... Sep 9-14
DAY 1: Advanced Attacks
As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We’ll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQLI server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers find ways to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

DAY 2: Web Frameworks
We’ll continue exploring advanced discovery and exploitation techniques for today’s complex web applications. We’ll look at vulnerabilities that could affect web applications written in any backend language, then examine how logic flaws in applications, especially in Mass Object Assignments, can have devastating effects on security. We’ll also dig into assumptions made by core development teams of backend programming languages and learn how even something as simple as handling the data types in variables can be leveraged through the web with Type Juggling and Object Serialization. Next we’ll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. Part of this discussion will lead us to cutting-edge technologies like the MEAN stack, where JavaScript is leveraged from the browser, web server, and backend NoSQL storage. The final section of the class examines applications in content management systems such as SharePoint and WordPress, which have unique needs and features that make testing them both more complex and more fruitful for the tester.

Topics: Web Architectures, Web Design Patterns; Languages and Frameworks; Java and Struts; PHP-Type Juggling; Logic Flaws; Attacking Object Serialization; The MEAN Stack; Content Management Systems; SharePoint; WordPress

DAY 3: Web Cryptography
Cryptographic weaknesses are common, yet few penetration testers have the skill to investigate, attack and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer, but do not inherently protect encrypted data from being attacked, or only permit the developer to use cryptography in a weak manner. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and hashing insecurely. Students will learn techniques ranging from identifying what the encryption technique is to exploiting various flaws within the encryption or hashing.

Topics: Identifying the Cryptography Used in the Web Application; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Collisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

DAY 4: Alternative Web Interfaces
Web applications are no longer limited to the traditional HTML-based interfaces. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. We will examine Flash, Java, ActiveX, and Silverlight vulnerabilities; SOAP and REST Web Services; Penetration Testing Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

Topics: Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

DAY 5: Web Application Firewall and Filter Bypass
Applications today are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. The controls block many of the automated tools and simple techniques used to discover flaws. On this day we’ll explore techniques used to map the control and how that control is configured to block attacks. You’ll be able to map out the rule sets and determine the specifics of how the Web Application Firewall detects attacks. This mapping will then be used to determine attacks that will bypass the control. You’ll use HTML5, UNICODE, and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding Web Application Firewaling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPES, and Data URLs to Bypass Restrictions; Bypassing a Web Application Firewall’s Best-Defended Vulnerabilities, XSS and SQLi

DAY 6: Capture the Flag
On this final course day you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You’ll be able to use these skills against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF). You will be able to use this both in the class and after leaving and returning to your job.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques
SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**

**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

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 day 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 day 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, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five 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 day 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.
Defeating ASLR on the Linux OS
Stack; Defeating Stack Protection on the Linux OS;
Performing Return-to-libc (ret2libc) Attacks on the
Stack-Based Overflows on the Linux OS;
Programming (ROP); Identifying and Analyzing
Redirection and Memory Leaks; Return-Oriented
Performing Symbol Resolution on the Linux OS;
a Binary and Analyzing x86 Assembly Code;
and Allocation on the Linux OS; Disassembling
Topics:
Perspective and Discuss the Topic of Privilege
Take a Look at the Linux OS from an Exploitation
Throughout the Remainder of the Course. We Will
Must Be Intimately Understood. Disassembly
Registers Are Directly Manipulated by Testers and
x86 Assembler and Linking and Loading. Processor
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; UsingROP; BuildingROP Chains
to Defeat DEP and Bypass ASLR; Windows 7
and 8, Porting Metasploit Modules; Client-side
Exploitation; Windows Shellcode

"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
SEC760: Advanced Exploit Development for Penetration Testers

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, 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 exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- How to utilize a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- 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 and defeating determination

Course Author Statement

“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

You Will Be Able To

- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- Perform remote debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows
- Write Return-Oriented Shellcode
- Perform patchdiffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows heap overflows and use-after-free attacks
- Use precision heap sprays to improve exploitability
- Perform Windows Kernel debugging up through Windows 8 64-bit
- Jump into Windows kernel exploitation

SEC760 is available via (subject to change):

Live Training

- SANSFIRE . . . . . . . . Washington, DC . . . . Jun 17-22
- Network Security . . . . Las Vegas, NV . . . . Sep 9-14

Summit Events

- Purple Team . . . . . . . . Las Colinas, TX . . . . Oct 23-28
- Pen Test HackFest . . . . Bethesda, MD . . . . Nov 20-25

Private Training

This course is also available through Private Training.
**Course Day Descriptions**

**DAY 1: Threat Modeling, Reversing and Debugging with IDA**
Many penetration testers, incident handlers, developers, and other related professionals lack reverse-engineering and debugging skills. These are different skills than reverse-engineering malicious software. As part of the Security Development Lifecycle (SDL) and Secure-SDLC, developers and exploit writers should have experience using IDA Pro to debug and reverse their code when finding bugs or when identifying potential risks after static code analysis or fuzzing.

**Topics:** Security Development Lifecycle, Threat Modeling, Why IDA Is the #1 Tool for Reverse Engineering, IDA Navigation, IDA Python and the IDA IDC, IDA Plug-ins and Extensibility, Local Application Debugging with IDA, Remote Application Debugging with IDA

**DAY 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 SEC660. Heap overflows serve as a rite of passage into modern exploitation techniques. This day is aimed at bridging this gap of knowledge in order to inspire thinking in a more abstract manner, necessary for continuing further with the course.

**Topics:** Linux Heap Management, Constructs, and Environment, Navigating the Heap, Exploiting Macros such as `unl ink` and `f rontlink`; Function Pointer Overwrites; Format String Exploitation; Accessing Custom Doubly-Linked Lists; Defeating Linux Exploit Mitigation Controls; Using IDA for Linux Application Exploitation; Using Format String Bugs for ASLR Bypass

**DAY 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 day 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)

**DAY 4: Windows Kernel Debugging and Exploitation**
The Windows Kernel is very complex and intimidating. This course day aims to help you understand the Windows Kernel and the various exploit mitigations added into recent versions. You will perform Kernel debugging on various versions of the Windows OS, such as Windows 7 and 8, and learn to deal with its inherent complexities. Exercises will be performed to analyze vulnerabilities, look at exploitation techniques, and get a working exploit.

**Topics:** Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel Protections; Debugging the Windows 7/8 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HL Dispatch Table Overwrites

**DAY 5: Windows Heap Overflows and Client-Side Exploitation**
The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ vtable overflows, one of the most common mechanisms used to compromise a modern Windows system. Many of these vulnerabilities are discovered in the browser, so browser techniques will also be taught, including modern heap spraying to deal with Internet Explorer 8/9/10 and other browsers such as Firefox and Chrome. You will work towards writing exploits in the Use-After-Free/Dangling Pointer vulnerability class.

**Topics:** Windows Heap Management, Constructs, and Environment; Understanding the Low Fragmentation Heap (LFH); Browser-based and Client-side Exploitation; Remedial Heap Spraying; Understanding C++ vtable/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

**DAY 6: Capture-the-Flag Challenge**
Day 6 will feature a Capture-the-Flag event with different types of challenges taken from material taught throughout the week.

**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

“SEC760 is the challenge I am looking for. It will be overwhelming, but well worth it.”

-William Stott, Raytheon

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

<table>
<thead>
<tr>
<th>6 Day Program</th>
<th>36 CPES</th>
<th>Laptop Required</th>
</tr>
</thead>
</table>

**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-stamped malware, along with utilityware 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.
- Identify compromised and affected systems.
- Detect how and when a breach occurred.
- 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.
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment.
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms.
- Target advanced adversary anti-forensics techniques like hidden and time-stamped malware, along with utilityware 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.

**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.

**FOR508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!”**

- Neel Mehta, Chevron

---

**FOR508 is available via (subject to change):**

<table>
<thead>
<tr>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kansas City</td>
<td>Jun 10-15</td>
</tr>
<tr>
<td>SANSFIRE</td>
<td>Jun 17-22</td>
</tr>
<tr>
<td>Rocky Mountain</td>
<td>Jul 15-20</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Aug 12-17</td>
</tr>
<tr>
<td>Virginia Beach</td>
<td>Aug 25-30</td>
</tr>
<tr>
<td>New York City</td>
<td>Aug 25-30</td>
</tr>
<tr>
<td>Las Vegas, NV</td>
<td>Sep 9-14</td>
</tr>
<tr>
<td>Reston, VA</td>
<td>Sep 30 - Oct 5</td>
</tr>
<tr>
<td>Seattle, WA</td>
<td>Oct 14-19</td>
</tr>
<tr>
<td>Coral Gables, FL</td>
<td>Nov 4-9</td>
</tr>
<tr>
<td>Atlanta, GA</td>
<td>Nov 18-23</td>
</tr>
<tr>
<td>Austin, TX</td>
<td>Nov 18-23</td>
</tr>
<tr>
<td>San Francisco, CA</td>
<td>Dec 2-7</td>
</tr>
<tr>
<td>Washington, DC</td>
<td>Dec 14-19</td>
</tr>
</tbody>
</table>

**Learn about how to respond to attack...”**

“...or the next one. This training is a must have.”

- Neel Mehta, Chevron

---

www.giac.org/gcfa

**GCFA**

**Forensic Analyst**

**NEW**

---

"FOR508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!”

- Neel Mehta, Chevron
Course Day Descriptions

**DAY 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” and 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

---

**DAY 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 trade-craft 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

---

**DAY 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 have 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 Endpoint Detection and Repose; Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

---

**DAY 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 forensic 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

---

**DAY 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-Forensics Detection; Anti-Forensics Detection Methodologies; Identifying Compromised Hosts without Active Malware

---

**DAY 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 week 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 hacktivist groups.

**Topics:** Identification and Scoping; Containment and Threat Intelligence Gathering, Remediation and Recovery

---

**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

---

**Summit Events**
- **Enterprise Defense Summit** – Redondo Beach, CA – June 5-10
- **DFIR Summit** – Austin, TX – July 27 - Aug 1
- **THIR Summit** – New Orleans, LA – Oct 2-7

---

**Private Training**
This course is also available through Private Training.

---

**Online Training**
**OnDemand**
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**
Online Training – July 27 - Aug 1

---

61
**FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**

**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.

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.

---

**Live Training**

<table>
<thead>
<tr>
<th>Summit Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFR</td>
</tr>
<tr>
<td>THIR</td>
</tr>
</tbody>
</table>

**Private Training**

This course is also available through Private Training.

**FOR572 is available via (subject to change):**

<table>
<thead>
<tr>
<th>SANSFIRE</th>
<th>Washington, DC</th>
<th>Jun 17-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDI</td>
<td>Washington, DC</td>
<td>Dec 14-19</td>
</tr>
<tr>
<td>Raleigh</td>
<td>Raleigh, NC</td>
<td>Sep 16-21</td>
</tr>
<tr>
<td>N. VA Fall – Reston</td>
<td>Reston, VA</td>
<td>Sep 30 - Oct 5</td>
</tr>
<tr>
<td>DFIRCON Miami</td>
<td>Coral Gables, FL</td>
<td>Nov 4-9</td>
</tr>
<tr>
<td>San Francisco Winter</td>
<td>San Francisco, CA</td>
<td>Dec 2-7</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 9-14</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Aug 12-17</td>
</tr>
</tbody>
</table>
### Course Day Descriptions

**DAY 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. Today 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

---

**DAY 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; Firewall, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; Elastic Stack and the SOF-ELK Platform

---

**DAY 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

---

**DAY 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); Commercial Network Forensics; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

---

**DAY 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

---

**DAY 6: Network Forensics Capstone Challenge**
This section will combine all of what you have learned prior to and during this week. 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

---

### 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

---

“I love how this course is very well organized, and how the step-by-step walk-through of the lab allows even someone new to network forensics to get started right away.”

-Paul Kim, PWC

---

### Online Training

**OnDemand**
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**
Online Training . . . . . . . . . . . . . . . . Jul 27 - Aug 1
FOR500: Windows Forensic Analysis

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- 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, geolocation, browser history, profile USB device usage, and more
- Uncover the exact time 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), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user 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 key Windows artifacts such as the Registry and log files
- Use event log analysis techniques 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

FOR500: Windows Forensic Analysis will teach you to:

- 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 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.

“I have gained so much insight taking this course and can’t wait to apply these skills!”

-Dylan Ong, Stroz Friedberg

FOR500 is available via (subject to change):

Live Training

| SANSFIRE | Washington, DC | Jun 17-22 |
| Pittsburgh | Pittsburgh, PA | Jul 8-13 |
| San Francisco Summer | San Francisco, CA | Jul 22-27 |
| Chicago | Chicago, IL | Aug 19-24 |
| Tampa-Clearwater | Clearwater, FL | Aug 25-30 |
| Virginia Beach | Virginia Beach, VA | Aug 25-30 |
| Network Security | Las Vegas, NV | Sep 9-14 |
| San Francisco Fall | San Francisco, CA | Sep 23-28 |
| Baltimore Fall | Baltimore, MD | Oct 7-12 |
| Denver | Denver, CO | Oct 14-19 |
| Santa Monica | Santa Monica, CA | Oct 21-26 |
| Orlando | Orlando, FL | Oct 28 - Nov 2 |
| Houston | Houston, TX | Oct 28 - Nov 2 |
| DEFIRCON Miami | Coral Gables, FL | Nov 4-9 |
| CDI | Washington, DC | Dec 14-19 |
Course Day Descriptions

DAY 1: Windows Digital Forensics and Advanced Data Triage
The Windows forensics 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. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

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

DAY 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 key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices. Throughout the section, investigators will use their skills in a real hands-on case, exploring and analyzing the evidence.

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; Tools Utilized

DAY 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

DAY 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. 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

DAY 5: Core Windows Forensics Part 4 – Web Browser Forensics: 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 has become 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 analyst will learn how to examine every significant artifact stored by the browser and 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.

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

DAY 6: Windows Forensic Challenge
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.

Topics: Digital Forensic Case; Windows 10 Forensic Challenge

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

“Anyone involved in digital investigations needs to take this class! It covers or touches upon almost every aspect of Windows forensic investigations in a very short period of time.”
-Cy Bleistine, NJSP

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

Simulcast
Online Training

Summit Events
Day 1: DFIR Austin, TX . Jul 27 - Aug 1
Day 3: Toronto, ON . Oct 9 - 15
Day 4: Montreal, QC . Oct 23 - 27
Day 6: Toronto, ON . Oct 9 - 15

Community Events
Seattle, WA . Jun 3-8
Tempe, AZ . Sep 22-27

Mentor Events
Seattle, WA . Jun 18 - Aug 6

Private Training
This course is also available through Private Training.
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.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense, hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

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.

**FORENSICATE DIFFERENTLY!**
Course Day Descriptions

**DAY 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; Disks & Partitions; iOS Essentials and iOS Acquisition

**DAY 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 day, students will review Mac and iOS triage data.

**Topics:** File System; Extended Attributes; File System Events Store Database; Spotlight; Mac and iOS Triage; Most Recently Used (MRU)

**DAY 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. 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

**DAY 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; Apple Pay, Wallet, Passes

**DAY 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:** Live Response; Time Machine, OS X Malware and Intrusion Analysis; iCloud, Versions; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

**DAY 6: Mac Forensics & Incident Response Challenge**
Students will put their new Mac forensics 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

---

**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

---

“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
FOR526: Advanced Memory Forensics & Threat Detection

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526: Memory Forensics In-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

MALWARE CAN HIDE, BUT IT MUST RUN

What You Will Receive

- SIFT Workstation 3
  - This course extensively uses the SIFT Workstation 3 to teach incident responders and forensic analysts how to respond to and investigate sophisticated attacks. SIFT contains hundreds of free and open-source tools, easily matching any modern forensic and incident response commercial tool suite.
  - Ubuntu LTS base
  - 64 bit-based system
  - Better memory utilization
  - Auto-DFIR package update and customizations
  - Latest forensic tools and techniques
  - VMware Appliance ready to tackle forensics
  - Cross-compatibility between Linux and Windows
  - Expanded filesystem support (NTFS, HFS, EXFAT, and more)

- Windows 8.1 Workstation with license
  - 64 bit-based system
  - A licensed virtual machine loaded with the latest forensic tools
  - VMware Appliance ready to tackle forensics

- 32 GB Course USB 3.0
  - USB loaded with memory captures, SIFT Workstation 3, tools, and documentation

- SANS Memory Forensics Exercise Workbook
  - Exercise book is over 200 pages long with detailed step-by-step instructions and examples to help you become a master incident responder

- SANS DFIR cheat sheets to help use the tools

- MP3 audio files of the complete course lecture

FOR526 is available via (subject to change):

Live Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANSFIRE</td>
<td>Washington, DC</td>
<td>Jun 17-22</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 9-14</td>
</tr>
</tbody>
</table>

Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFIR</td>
<td>Austin, TX</td>
<td>Jul 27 - Aug 1</td>
</tr>
<tr>
<td>THIR</td>
<td>New Orleans, LA</td>
<td>Oct 2-7</td>
</tr>
</tbody>
</table>

Private Training

This course is also available through Private Training.

Online Training

OnDemand

Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

Simulcast

Online Training. Jul 27 - Aug 1
Course Day Descriptions

**DAY 1: Foundations in Memory Analysis and Acquisition**
Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first piece of the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

**Topics:** Why Memory Forensics? Investigative Methodologies; The Ubuntu SIFT and Windows 10 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

---

**DAY 2: Unstructured Analysis and Process Exploration**
Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.

**Topics:** Unstructured Memory Analysis; Page File Analysis; Examining Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects

---

**DAY 3: Investigating the User via Memory Artifacts**
An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.

**Topics:** Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory

---

**DAY 4: Internal Memory Structures**
Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, “Spotting Rootkit Behaviors” and “Extracting Suspicious Binaries,” it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

**Topics:** Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files

---

**DAY 5: Memory Analysis on Platforms Other than Windows**
Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac—that is, platforms other than Windows.

**Topics:** Linux Memory Acquisition and Analysis; Mac Memory Acquisition and Analysis

---

**DAY 6: Memory Analysis Challenges**
This final course section provides students with a direct memory forensics challenge that makes use of the DFIR NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen students’ ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

**Topics:** Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OS X Memory Image Parsing; Windows Hibernation Files Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)

---

Who Should Attend

- Incident response team members
- Experienced digital forensic analysts
- Red team members, penetration testers, and exploit developers
- Law enforcement officers, federal agents, and detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

---

“This training is a must for learning the foundations of memory forensics and becoming efficient at it. Highly recommended.”

-Hugo Gabignon, Amazon

---

"FOR526 is the best training I've had in years. I'm learning many new tools and methodologies and using them in labs immediately."

-Josh Burbank, Northrop Grumman
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
DAY 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, the day 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; Understanding Cyber Threat Intelligence; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

DAY 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: Intrusion Analysis; Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware

DAY 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

DAY 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

DAY 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

“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
FOR585: Smartphone Forensic Analysis In-Depth

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

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!

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 just 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.

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. The course features 27 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.

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!
Course Day Descriptions

DAY 1: Smartphone Overview, Misfit Devices, SQLite Introduction, and Android Forensics Overview

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. On this first course day, students will apply what they know to smartphone forensic handling, device capabilities, acquisition methods, misfit devices, SQLite database examination, and query development. They’ll also gain an overview of Android devices and manually crack locked Androids. Students will become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. We realize that not everyone examines BlackBerry and knock-off devices, which is why we offer “choose your own adventure” labs, meaning that students can select the labs most relevant to them. BlackBerry 10 smartphones are designed to protect user privacy, but techniques taught on this course day will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of BlackBerry 10 device file systems. Knock-off devices are another outlier than can be parsed and decoded once you become familiar with the file system structures.

Topics: The SIFT Workstation; Introduction to Smartphones; Smartphone Handling; Forensic Acquisition Concepts of Smartphones; Smartphone Components; Smartphone Forensic Tool Overview; BlackBerry 10 Forensics; Introduction to SQLite; Android Forensic Overview; Handling Locked Android Devices

DAY 2: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come 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; Android Evidentiary Locations; Traces of User Activity on Android Devices; Android Backup Files; Google Cloud Data and Extractions

DAY 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 for bypassing locked iOS devices and correctly interpreting the data. 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

DAY 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 class. Up to five labs will be conducted on this day alone! The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped smartphone.

Topics: iOS Backup File Forensics; Locked iOS Backup Files; iCloud Data Extraction and Analysis; Malware and Spyware Forensics; Detecting Evidence Destruction

DAY 5: Third-Party Application Analysis

This day 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 day 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 you 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

DAY 6: Smartphone Forensics Capstone Exercise

This final course day 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

“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

Online Training

OnDemand

Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

Simulcast

Online Training . . . . . . . . . . . . . . . . . . . . . . Jul 27 - Aug 1

73
FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**

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.

---

**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

**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

---

**FOR610 is available via (subject to change):**

**Live Training**

- **SANSFIRE**
  - **Washington, DC**
  - **Jun 17-22**
- **New York City**
  - **New York, NY**
  - **Aug 25-30**
- **Network Security**
  - **Las Vegas, NV**
  - **Sep 9-14**
  - **N. VA Fall – Reston**
  - **Reston, VA**
  - **Sep 30 - Oct 5**
- **Baltimore Fall**
  - **Baltimore, MD**
  - **Oct 7-12**
- **DFIRCON Miami**
  - **Coral Gables, FL**
  - **Nov 4-9**
- **CDI**
  - **Washington, DC**
  - **Dec 14-19**

**Summit Events**

- **DFIR**
  - **Austin, TX**
  - **Jul 27 - Aug 1**
- **THIR**
  - **New Orleans, LA**
  - **Oct 2-7**

**Private Training**

This course is also available through Private Training.
Forensics for Malware Analysis

Analyzing Multi-Technology and Fileless Malware; Started with Unpacking; Using Debuggers

Recognizing Packed Malware; Getting hooked, examining this functionality from both physical and file system. Code analysis focuses on the specimen’s code and makes use of a disassembler and debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner, and set up such a lab on your laptop using the supplied Windows and Linux (Remnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab—with guidance and explanations from the instructor—to reinforce the concepts discussed throughout the day.

Topics: Assembling a Toolkit for Effective Malware Analysis; Examining Static Properties of Suspicous 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

DAY 2: Reversing Malicious Code

Section two focuses on examining malicious Windows executables at the assembly level. You will discover approaches for studying inner workings of a specimen by looking at it through a disassembler and, at times, with the help of a debugger. 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 incorporate 64-bit malware, given its growing popularity. 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

DAY 3: Malicious Web and Document Files

Section three 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 de-obfuscate malicious scripts with the help of script debuggers and interpreters, examine 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 JavaScript; Dissecting Malicious JavaScript Using Debuggers and Interpreters; Analyzing Suspicious PDF Files; Examining Malicious Microsoft Office Documents, Including Files with Macros; Analyzing Malicious RTF Document Files

DAY 4: In-Depth Malware Analysis

Section four 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 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

DAY 5: Examining Self-Defending Malware

Section five takes a close look at the techniques malware authors commonly employ 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 Pack’s Actions

DAY 6: Malware Analysis Tournament

Section six assigns students to the role of a malware analyst working as a member of an incident response or forensics team. Students are presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a student’s ability to respond to typical malware-reversing tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, the challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular DFIR NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shore up skill areas where they feel they need additional practice. Students who score the highest in the malware analysis challenge will be awarded the coveted SANS Lethal Forensicator coin.

Topics: Behavioral Malware Analysis; Dynamic Malware Analysis (Using a Disassembler); Static Malware Analysis (Using a Debugger), Static Malware Analysis; Identifying common characteristics at a code level, including HTTP command and control, keylogging, and command execution.

“"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
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.

Author 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 8 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 8 domains of knowledge!”

- Eric Conrad and Seth Misenar

“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
Course Day Descriptions

**DAY 1: Introduction; Security and Risk Management**

On the first day 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

---

**DAY 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 today’s course section, 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 2019 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)

---

**DAY 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

---

**DAY 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

---

**DAY 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 day five with a deep dive into disaster recovery.

**Topics:** Domain 6: Security Assessment; Domain 7: Security Operations

---

**DAY 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

---

**Community Events**

- Austin, TX ................................. Jul 8-13
- Atlanta, GA ............................... Jul 22-27
- Chicago, IL ............................... Aug 12-17
- St. Louis, MO ............................. Aug 19-24

**Private Training**

This course is also available through Private Training.

---

**Who Should Attend**

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

---

“Great discussions and examples that provide a clear understanding and relate material to examples.”

-Kelley ONeil, Wells Fargo

---

**Online Training**

**OnDemand**

Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**

Online Training ................................ Jul 15-20
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.

- **Develop Strategic Plans**
  Strategic planning is hard for IT and IT 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 your response was, “No way, I am not going to do that!” Policy must be aligned with an organization’s culture. We will break down the steps to policy development so that you have the ability to design and assess policy to 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 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 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 have the fundamental skills to create strategic plans that protect your company, enable key innovations, and facilitate working effectively with your business partners.

“**This course provided a full scope of leadership and security that can immediately be applied to your job.”**

-Jerry Butler, NAVSEA OOI
### Day 1: Strategic Planning Foundations
Creating security-strategic plans requires a fundamental understanding of the business, and a deep understanding of the threat landscape.

**Topics:** Vision and Mission Statements; Stakeholder Management; PEST Analysis; Porter’s Five Forces; Threat Actors; Asset Analysis; Threat Analysis

### Day 2: Strategic Roadmap Development
With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, 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 do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

**Topics:** Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications

### Day 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. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach the techniques to create successful policy that employees will read and follow, and that will be accepted by business units. Students will learn key elements of policy, including positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment.

**Topics:** Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training

### Day 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 how to develop from a manager into a leader.

**Topics:** Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development

### Day 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 Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management

---

**Who Should Attend**
- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

---

**Outstanding.”**
- Jeff Haynes, NELO
This course is offered by the SANS Institute as a PMI® Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. PMP® is a registered trademark of Project Management Institute, Inc.

This course has recently been updated to fully prepare you for changes in the 2019 PMP® exam. 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 – Sixth Edition 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, and to completing, closing, and documenting as your project finishes.

A copy of the PMBOK® Guide – Sixth Edition 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 updated 2019 Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

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.

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
**DAY 1: Project Management Structure and Framework**

This course day 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

---

**DAY 2: Project Charter and Scope Management**

During day two, 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 your project is well defined from the outset. 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

---

**DAY 3: Schedule and Cost Management**

Our third day 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

---

**DAY 4: Communications and Project Resources**

During day four, 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 day 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

---

**DAY 5: Quality and Risk Management**

On day five you will become familiar with quality planning, assurance, and control methodologies, as well as learn 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 how to understand and use quality control charts. The risk section goes over known versus 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 how 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

---

**DAY 6: Procurement, Stakeholder Management, and Project Integration**

We close out the week 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
One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked 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 we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized 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, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

You’ll be able to use what you learn immediately. Five of the six days in the course will help you produce your own checklist, or provide you with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the six hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

“AUD507 provides insight on different aspects related to system configurations and associated risks.”

-Yosra Al-Basha, Yemen LNG Co.
Course Day Descriptions

**DAY 1: Effective Auditing, Risk Assessment & Reporting**

After laying the foundation for the role and function of an auditor in the information security field, this day’s material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and help you to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions when dealing with virtualization and cloud computing.

**Topics:** Auditor’s Role; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization & Cloud Computing

**DAY 2: Effective Network & Perimeter Auditing/Monitoring**

Enterprise networks are under constant assault. A key foundation in the security of our enterprise is created by ensuring that we have a validated secure perimeter. As easy as this is to say, organizations struggle with this constantly. Forces such as wireless technologies, enterprise VPNs, business partner connections, BYOD policies and more can all erode the security of our perimeter networks. On this day we will build from the ground up, dealing with security controls, proper deployment, effective auditing continuous monitoring of configuration from Layer 2 all the way up the stack. Students will learn how to identify insecurely configured VLANs, how to determine perimeter firewall requirements, how to examine enterprise routers and much more.

**Topics:** Secure Layer 2 Configurations; Router & Switch Configuration Security; Firewall Auditing; Validation & Monitoring; Wireless; Network Population Monitoring; Vulnerability Scanning

**DAY 3: Web Application Auditing**

A portion of the morning will cover all of the underlying principles of web technology and introduce a set of tools that can be used to validate the security of these applications. Throughout the day, all of the OWASP Top Ten issues will be addressed, abstracted into five practical principles of web application design and deployment. The majority of the day will be spent building and working through a checklist for validating the existence and proper implementation of controls to mitigate the primary threats found in web applications through the use of cutting-edge techniques and advanced testing methods. Throughout the day, time is spent identifying key development requirements, allowing you to provide meaningful feedback into your organization’s coding standards.

**Topics:** Identifying Controls Against Information Gathering Attacks; Processing Controls to Prevent Hidden Information Disclosures; Controlling Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identifying Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

**DAY 4: Advanced Windows Auditing & Monitoring**

During the course of this day, attendees will have the opportunity to perform a thorough hands on audit of Active Directory servers in class, in addition to the laptop that they bring to class. In addition to covering all of the major audit points in a stand-alone Windows system, the course will scale these methods for use within a domain. One of the primary goals of the material presented is to allow the auditor to get away from checking registry settings, helping administrators to create a comprehensive management process that automatically verifies settings. With this type of system in place, the auditor can step back and begin auditing the management processes which generally helps us to be far more effective.

**Topics:** Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

**DAY 5: Advanced UNIX Auditing & Monitoring**

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as access controls and security models. Most of the day will be spent working hands-on with the instructor to create a comprehensive set of auditing scripts that can be used on virtually any Unix system. This set of scripts can be used to either check the security of a system, report on the compliance of the system to a baseline or be used in a change control process to validate a system before patching and subsequently re-generate the system baseline.

**Topics:** Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

**DAY 6: Audit the Flag: A NetWars Experience**

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course. This allows students to immediately put the knowledge gained into practice with these guided challenges. At the conclusion of the day, students are asked to identify the most serious findings within the enterprise environment and to suggest possible root causes and potential mitigations.

**Topics:** Network Devices; Servers; Applications; Workstations

**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
LEG523: Law of Data Security and Investigations

**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).

**LEG523 is available via (subject to change):**

**Live Training**
- SANSFIRE .......... Washington, DC .......... Jun 17-21
- Crystal City .......... Arlington, VA .......... Aug 5-9

**Private Training**
This course is also available through Private Training.

**Online Training**

**OnDemand**
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**vLive**
Online Training .......... Jun 25 - Aug 1

**Simulcast**
Online Training .......... Sep 9-13

**LEG523**

**I wish I’d taken LEG523 four years ago, so that our policy and governance could have been enhanced sooner.”**

-Tom Siu,
Case Western Reserve University

LEG523 is constantly updated to address changing trends and current events. Here’s a sampling of what’s new:

- The global imperative for organizations to demonstrate a culture of data privacy.
- Invoking attorney-client privilege to maintain confidentiality of security assessments such as pen tests.
- Court decision shows how to improve an official investigation using artificial intelligence.
- Unique and indispensable training for General Data Protection Regulation (GDPR) Data Protection Officers.
- Form contract for inviting outside incident responders - including police, contractors, National Guard, or civil defense agency anywhere in the world - to help with a cyber crisis.
- The EU’s new GDPR and its impact around the world.

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 IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and records management procedures.

This course covers the law of fraud, crime, policy, contracts, liability, IT security 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.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

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. Non-U.S. professionals 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.

For example, a lawyer from the national tax authority in an African country took the course.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals 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.

**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 the like).
Course Day Descriptions

DAY 1: Fundamentals of Data Security Law and Policy

The first day is an introduction to law and IT that serves as the foundation for discussions during the rest of the course. We survey the general legal issues that must be addressed when a company is thinking about implementing an information security program, as well as emerging topics such as honeypots. We will look at the impact of future technologies on law and investigations in order to help students factor in legal concerns when they draft enterprise IT security policies. For example, students will debate what the words of an enterprise policy would mean in a courtroom. The course also dives deep into the legal question of what constitutes a “breach of data security” for purposes of notifying others about it or for other purposes. The course includes a case study on the drafting of policy to comply with the Payment Card Industry Data Security Standard (PCI). Students learn how to choose words more carefully and accurately when responding to cybersecurity questionnaires from regulators, cyber insurers and corporate customers.

DAY 2: E-Records, E-Discovery and Business Law

IT professionals can advance their careers by upgrading their expertise in the hot fields of e-discovery and cyber investigations. Critical facets of those fields come forward in course day two. We will focus on the use of computer records in disputes and litigation, with a view to teaching students how to manage requests to turn over e-records to adversaries (i.e., e-discovery), manage implementation of a “legal hold” over some records to prevent their destruction, and coordinate with legal counsel to develop workable strategies to legal challenges. Transactions that used to be conducted on paper are now done electronically, so commercial law now applies to computer security. The IT function within an enterprise has become the custodian of an enterprise’s business records. You will learn how to craft sound policy for the retention and destruction of electronic records like email, text messages, and social networking interactions. We will provide methods for balancing the competing interests in electronic records management, including costs, risks, security, regulations and user cooperation. Law and technology are changing quickly, and it is impossible for professionals to comprehend all the laws that apply to their work. But they can comprehend overarching trends in law, and they can possess a mindset for finding solutions to legal problems. A key goal of this course day is to equip students with the analytical skills and tools to address technology law issues as they arise, both in the United States and around the world. Special attention is devoted to European data protection laws (see the white paper by Mr. Wright on the European Union’s new General Data Protection Regulation). The course is chock full of actual court case studies dealing with privacy, computer records, digital evidence, electronic contracts, regulatory investigations, and liability for shortfalls in security. The purpose of the case studies is to draw practical lessons that students can take back to their jobs.

DAY 3: Contracting for Data Security and Other Technology

Day three focuses on the essentials of contract law sensitive to the current legislative requirements for security. Compliance with many of the new data security laws requires contracts. Because IT pulls together the products and services of many vendors, consultants, and outsourcers, enterprises need appropriate contracts to comply with Gramm-Leach-Bliley, HIPAA, GDPR, PCI-DSS, data breach notice laws and other regulations. The course provides practical steps and tools that students can apply to their enterprises and includes a lab on writing contract-related documents relevant to the students’ professional responsibilities. (The lab is an optional, informal “office hours” discussion with the instructor at the end of the day when the course is delivered live.) You will learn the language of common technology contract clauses and the issues surrounding those clauses, and become familiar with specific legal cases that show how different disputes have been resolved in litigation. Recognizing that enterprises today operate increasingly on a global basis, the course teaches cases and contract drafting styles applicable to a multinational setting. Contracts covered include agreements for software, consulting, nondisclosure, outsourced services, penetration testing, and private investigation services (such as cyber incident response). Special emphasis is applied to cloud computing issues. Students will also learn how to exploit the surprising power of informal contract records and communications, including cybersecurity questionnaires and requests for InfoSec assurances.

DAY 4: The Law of Data Compliance: How to Conduct Investigations

Information security professionals and cyber investigators operate in a world of ambiguity, rapid change, and legal uncertainty. To address these challenges, this course day presents methods to analyze a situation and then act in a way that is ethical and defensible and reduces risk. Lessons will be invaluable to the effective and credible execution of any kind of investigation, be it internal, government, consultant, security incident, or any other. The lessons also include methods and justifications for maintaining the confidentiality of an investigation. The course surveys white-collar fraud and other misbehaviors with an emphasis on the role of technology in the commission and prevention of that fraud. It teaches IT managers practical and case-study-driven lessons about the monitoring of employees and employee privacy. IT is often expected to “comply” with many mandates, whether stated in regulations, contracts, internal policies or industry standards (such as PCI-DSS). This course teaches many broadly applicable techniques to help technical professionals establish that they and their organizations are in fact in compliance, or to reduce risk if they are not in perfect compliance. The course draws lessons from models such as the Sarbanes-Oxley Act. As IT security professionals take on more responsibility for controls throughout an enterprise, it is natural that they worry about fraud, which becomes a new part of their domain. This day covers what fraud is, where it occurs, what the laws say about it and how it can be avoided and remedied. Indeed, the primary objective of Sarbanes-Oxley is not to keep hackers out; it is to snuff out fraud inside the enterprise. Scattered through the course are numerous descriptions of actual fraud cases involving technology. The purpose is to acquaint the student with the range of modern business crimes, whether committed by executives, employees, suppliers or whole companies. More importantly, the course draws on the law of fraud and corporate misconduct to teach larger and broader lessons about legal compliance, ethical hacking and proper professional conduct in difficult case scenarios. Further, the course teaches how to conduct forensics investigations involving social, mobile and other electronic media. Students learn how to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event.

DAY 5: Applying Law to Emerging Dangers: Cyber Defense

Knowing some rules of law is not the same as knowing how to deal strategically with real-world legal problems. This day is organized around extended case studies in security law: break-ins, investigations, piracy, extortion, rootkits, phishing, botnets, espionage and defamation. The studies lay out the chronology of events and critique what the good guys did right and what they did wrong. The goal is to learn to apply principles and skills to address incidents in your day-to-day work. The course includes an in-depth review of legal responses to the major security breaches at TJOX, Target, and Home Depot, and looks at how to develop a Bring Your Own Device (BYOD) policy for an enterprise and its employees. The skills learned are a form of crisis management, with a focus on how your enterprise will be judged in a courtroom, by a regulatory agency, or in a contract relationship. Emphasis will be on how to present your side of a story to others, such as law enforcement, Internet gatekeepers, or the public at large, so that a security incident does not turn into a legal fiasco. In addition to case studies, the core material will include tutorials on relevant legislation and judicial decisions in such areas as privacy, negligence, contracts, e-investigations, computer crime and offensive countermeasures. LEGS23 is increasingly global in its coverage, so although this course day centers around U.S. law, non-U.S. law and the roles of government authorities outside the United States will be examined, as well. At the end of this course section, the instructor will discuss a few sample questions to help students prepare for the GIAC exam at the close of this course (GLEG).
This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization’s web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It 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 better defending their 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:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.
Course Day Descriptions

**DAY 1: Web Basics and Authentication Security**
We begin day one with an overview of recent web application attack and security trends, then follow up by examining the essential technologies that are at play in web applications. You cannot win the battle if you do not understand what you are trying to defend. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

**Topics:** HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

**DAY 2: Web Application Common Vulnerabilities & Mitigations**
Since the Internet does not guarantee the secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. This course day covers the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security.

**Topics:** SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-site Request Forgery; Business Logic Flaws; Concurrency; Input-related Flaws and Related Defenses; SQL Injection Vulnerabilities; Testing, and Defense

**DAY 3: Proactive Defense and Operation Security**
Day three begins with a detailed discussion on cross-site scripting and related mitigation and testing strategies, as well as HTTP response splitting. The code in an application may be totally locked down, but if the server setting is insecure, the server running the application can be easily compromised. Locking down the environment is essential, so we cover this basic concept of defending the platform and host. To enable any detection of intrusion, logging and error handling must be done correctly. We will discuss the correct approach to handling incidents and logs, then dive even further to cover the intrusion detection aspect of web application security. In the afternoon we turn our focus to the proactive defense mechanism so that we are ahead of the bad guys in the game of hack and defend.

**Topics:** Cross-site Scripting Vulnerability and Defenses; Web Environment Configuration Security; Intrusion Detection in Web Applications; Incident Handling; Honeytoken

**DAY 4: AJAX and Web Services Security**
Day four is dedicated to the security of asynchronous JavaScript and XML (AJAX) and web services, which are currently the most active areas in web application development. Security issues continue to arise as organizations dive head first into insecurely implementing new web technologies without first understanding them. We will cover security issues, mitigation strategies, and general best practices for implementing AJAX and web services. We will also examine real-world attacks and trends to give you a better understanding of exactly what you are protecting against. Discussion focuses on the web services in the morning and AJAX technologies in the afternoon.

**Topics:** Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

**DAY 5: Cutting-Edge Web Security**
Day five focuses on cutting-edge web application technologies and current research areas. Topics such as clickjacking and DNS rebinding are covered. These vulnerabilities are difficult to defend and multiple defense strategies are needed for their defense to be successful. Another topic of discussion is the new generation of single-sign-on solutions such as OpenID. We cover the implications of using these authentication systems and the common “gotchas” to avoid. With the adoption of Web2.0, the use of Java applet, Flash, ActiveX, and Silverlight is on the increase. The security strategies of defending these technologies are discussed so that these client-side technologies can be locked down properly.

**Topics:** Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single-Sign-On Solution and Security; IPv6 Impact on Web Security

**DAY 6: Capture-and-Defend-the-Flag Exercise**
Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. But the focus is 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, and 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 the operating system, the web server, finding configuration problems in the application language setup, and finding and fixing coding problems in the site.

**Topics:** Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation

---

**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

---

**Online Training**

**OnDemand**
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**

Online Training .............................. Sep 9-14

---

“Brilliant! The combination of hands-on exercises and Q&A streamlines learning like nothing else.”

~McKell Gomm, Henry Schein
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 the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management (“infrastructure as Code”), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and 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, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software. DEV540 provides in-depth analysis of the Amazon Web Services (AWS) toolchain, while lightly covering comparable services in Microsoft Azure. Using the CI/CD toolchain, students build a cloud infrastructure that can host containerized applications and microservices. Hands-on exercises analyze and fix cloud infrastructure and application vulnerabilities using security services and tools such as API Gateway, Identity and Access Management (IAM), CloudFront Signing, Security Token Service (STS), Key Management Service (KMS), managed WAF services, serverless functions, CloudFormation, AWS Security Benchmark, and much more.

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
**DAY 1: Introduction to Secure DevOps**

The first day is an introduction to DevOps practices, principles and tooling, how DevOps works, and how work is done in DevOps. We’ll look at the importance of culture, collaboration, and automation in DevOps. Using case studies of DevOps “Unicorns” – the Internet tech leaders who have created the DNA for DevOps – we’ll show you how and why they succeeded. This includes the keys to their DevOps security programs. Then you’ll learn Continuous Delivery – the automation engine in DevOps – and how to build up a Continuous Delivery or Continuous Deployment pipeline. This includes how security controls can be folded into or wired into the CD pipeline, and how to automate security checks and tests in CD.

**Topics:** Introduction to DevOps; Case Studies on DevOps Unicorns; Working in DevOps; Security Challenges in DevOps; Building a CD Pipeline; Securing Department Data; Security in Commit; Security in Pre-Commit; Security in Acceptance

---

**DAY 2: Moving to Production**

Building on the ideas and frameworks developed in the first course section, you will learn how secure Infrastructure as code using modern automated configuration management tools like Puppet, Chef and Ansible, allows you to quickly and consistently deploy new infrastructure and manage configurations. Because the automated CD pipeline is so critically important to DevOps, you’ll also learn to secure the pipeline, including RASP and other run-time defense technologies. As the infrastructure and application code moves to production, we’ll spend the second half of the day exploring container security issues associated with tools such as Docker and Kubernetes, as well as how to protect secrets using Vault and how to build continuous security monitoring using Graphana, Graphite, and StatsD. Finally, we’ll discuss how to build compliance into Continuous Delivery, using the security controls and guardrails that have been built in the DevOps toolchain.

**Topics:** Secure Infrastructure as Code; Security with Puppet Lab; Securing Your CD Pipeline; Threat Modeling and Locking Down Your Build and Deployment Environment; Run-Time Defense; Container Security; Security in Monitoring; Red Teaming; Bug Bounties and Blameless Postmortems; Managing Secrets; Compliance as Code

---

**DAY 3: Moving to the Cloud**

Observing DevOps principles, you’ll learn to deploy infrastructure, applications, and the CI/CD toolchain into the cloud. This section provides an overview of Amazon Web Services (AWS) and introduces the foundational tools and practices you’ll need to securely deploy your applications in the cloud.

**Topics:** Introduction to the Cloud, Cloud Architecture Overview; Secure Cloud Deployment; Security in CI/CD

---

**DAY 4: Cloud Application Security**

In this section, you’ll learn how to leverage cloud application security services to ensure that applications have appropriate encryption, authentication, authorization, and access control, while also maintaining functional and high-availability systems.

**Topics:** Data Protection; Secure Content Delivery; Microservice Security; Serverless Security

---

**DAY 5: Cloud Security Automation**

Expanding on the foundation of the previous sections, we’ll now focus on leveraging cloud services to automate security tasks such as deploying application patches to blue/green environments, deploying and configuring cloud web application firewalls, enabling cloud security monitoring, and automating cloud compliance scanning.

**Topics:** Blue/Green Deployment Options; Security Automation; Security Monitoring; Cloud Compliance

---

**Who Should Attend**

- Anyone working in the DevOps environment or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
- Anyone interested in learning how to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in learning how to leverage cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

---

**Community Events**

Atlanta, GA ................................. Jun 3-7
Vancouver, BC ............................. Jun 10-14
Seattle, WA ................................. Jun 17-21
Chicago, IL ................................. Jul 8-12
Portland, OR ............................... Sep 23-27

---

**Online Training**

**OnDemand**

Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

**Simulcast**

Complete this course on one of the scheduled dates. The schedule above lists the locations and dates for the Simulcast training.

Online Training ............................. Jun 17-21
Online Training ............................. Aug 12-16
This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- Identify security defects in your code
- Fix security bugs using secure coding techniques
- Utilize secure HTTP headers to prevent attacks
- Secure your sensitive representational state transfer (REST) services
- Incorporate security into your development process
- Use freely available security tools to test your applications

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a high-level theory course – it is about real-world, hands-on programming. You will examine actual code, work with real tools, build applications and gain confidence in the resources you need to improve the security of Java applications.

The course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques that you have learned in course.

PCI Compliance
Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. This is the course for you if your application processes cardholder data and you are required to meet PCI compliance.

Who Should Attend
- Developers who want to build more secure applications
- Java Enterprise Edition programmers
- Application security auditors
- Software engineers
- Technical project managers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

This course is also available through Private Training.
ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. However, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET 2.0, Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the responsibility is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

Have you ever wondered if the built-in ASP.NET validation is effective? Have you been concerned that Windows Communication Foundation (WCF) services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework?

This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

Rather than teaching students to use a set of tools, the course teaches students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates with a security review of a real-world open-source application. Students will conduct a code review, review a penetration test report, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that they have learned in class, implement fixes for these issues.

PCI Compliance
Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. This is the course for you if your application processes cardholder data and you are required to meet PCI compliance.

Who Should Attend
- ASP.NET developers who want to build more secure web applications
- .NET framework developers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers

“Very important course to learn how to avoid hacks!”
-Ahmed Zakaria, Thiqah

DEV544: Secure Coding in .NET: Developing Defensible Applications

You Will Be Able To
- Use a web application proxy to view HTTP requests and responses.
- Review and perform basic exploits of common .NET web application vulnerabilities, such as those found in the SANS/CWE Top 25 and the OWASP Top 10:
  - Cross-Site Scripting
  - Parameter Manipulation
  - Open Redirect
  - Unvalidated Forwards
  - SQL Injection
  - Session Hijacking
  - Clickjacking
  - Cross-Site Request Forgery
  - Man-in-the-middle (MITM)
- Mitigate common web application vulnerabilities using industry best practices in the .NET framework, including the following:
  - Input Validation
  - Blacklist & Whitelist Validation
  - Regular Expressions
  - Command Encoding
  - Output Encoding
  - Content Security Policy
  - Client-side Security Headers
- Understand built-in ASP.NET security mechanisms, including the following:
  - AntiForgeryToken
  - Data Annotations
  - Event Validation
  - Request Validation
  - View State
  - Entity Framework
  - ASP.NET Identity
  - Forms Authentication
  - Membership Provider
  - WCF
  - Web API
  - Roslyn Diagnostic Analyzers
- Apply industry best practices (NIST, PCI) for cryptography and hashing in the .NET framework
- Implementing a secure software development lifecycle (SDLC) that includes threat modeling, static analysis, and dynamic analysis

DEV544 is available via (subject to change):

Live Training
Private Training
This course is also available through Private Training.

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
ICS410: ICS/SCADA Security Essentials

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

Live Training

<table>
<thead>
<tr>
<th>Location</th>
<th>City, State</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANSFIRE</td>
<td>Washington, DC</td>
<td>Jun 17-21</td>
</tr>
<tr>
<td>Pittsburgh</td>
<td>Pittsburgh, PA</td>
<td>Jul 8-12</td>
</tr>
<tr>
<td>San Francisco Summer</td>
<td>San Francisco, CA</td>
<td>Jul 22-26</td>
</tr>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 9-13</td>
</tr>
<tr>
<td>San Diego</td>
<td>San Diego, CA</td>
<td>Oct 7-11</td>
</tr>
<tr>
<td>Denver</td>
<td>Denver, CO</td>
<td>Oct 14-18</td>
</tr>
<tr>
<td>Orlando</td>
<td>Orlando, FL</td>
<td>Oct 28 - Nov 1</td>
</tr>
<tr>
<td>Nashville</td>
<td>Nashville, TN</td>
<td>Dec 2-6</td>
</tr>
<tr>
<td>CDI</td>
<td>Washington, DC</td>
<td>Dec 14-18</td>
</tr>
<tr>
<td>Summit Events</td>
<td>Oil &amp; Gas Cybersecurity</td>
<td>Houston, TX</td>
</tr>
<tr>
<td>Private Training</td>
<td>This course is also available through Private Training.</td>
<td></td>
</tr>
</tbody>
</table>
Course Day Descriptions

DAY 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; Purdue Levels 0 and 1; Purdue Levels 2 and 3; DCS and SCADA; IT & ICS Differences; Physical and Cybersecurity; Secure ICS Network Architectures

DAY 2: Field Devices and Controllers
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 day 2, students will develop a better understanding of where these specific attack vectors exist and how to block them, starting at the lowest levels of the control network. 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 day 1 and look at what other fieldbus protocols are used in the industry. Later in the day, 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.

Topics: ICS Attack Surface; Purdue Levels 0 and 1; Ethernet and TCP/IP

DAY 3: Supervisory Systems
Day 3 will take students through the middle layers of control networks. 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. 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 interfaces and interfaces susceptible to password brute force attacks.

Topics: Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses; Exercise: Network Forensics of an Attack; Purdue Level 2 and 3 Attacks

DAY 4: Workstations and Servers
Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. 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 explore attacks and defenses on remote access for control systems.

Topics: Patching ICS Systems; Defending Microsoft Windows; Defending Unix and Linux; Endpoint Security Software; Event Logging and Analysis; Remote Access Attacks

DAY 5: ICS Security Governance
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. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. 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.

Topics: Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Disaster Recovery; Measuring Cybersecurity Risk; Incident Response; Exercise: Incident Response Tabletop Exercise; Final Thoughts and Next Steps

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

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
This five-day 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**

*Essentials for NERC Critical Infrastructure Protection*

**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!
DAY 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. On day 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 day 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

DAY 2: Access Control and Monitoring
Strong physical and cyber access controls are at the heart of any good cybersecurity program. During day 2 we move beyond the “what” of CIP compliance to understanding the “why” and the “how.” Firewalls, proxies, gateways, IDSs and more – learn where and when they help and learn practical implementations to consider and design 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 the learnings throughout the day 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

DAY 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 day 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 day 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

DAY 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. On day 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 on day 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

DAY 5: CIP Process
On the final day students will learn the key components for running an effective CIP compliance program. We will review the NERC processes for standards development, violation penalty determination, 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 day 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 on day 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

Course Day Descriptions
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 in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

This 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. An active defense is the approach needed to counter advanced adversaries targeting an ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. 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 malware analysis and incident response to ensure the safety and reliability of operations. The strategy 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 industrial control system (ICS) incident response focusing on security operations and prioritizing the safety and reliability of operations
- Determine 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 how to monitor ICS hotspots for abnormalities and threats. Methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape will be introduced and reinforced.
- Analyze ICS malware 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 when operations must shut down, or if it is safe to respond to the threat and continue operations.
- Use multiple security disciplines in conjunction with each other to leverage an active defense and safeguard the ICS, all reinforced with hands-on labs and technical concepts.

ICS515 is available via (subject to change):

**Live Training**

- **SANSFIRE**  Washington, DC  Jun 17-21
- **Columbia**  Columbia, MD  Jul 15-19
- **Network Security**  Las Vegas, NV  Sep 9-13

**Summit Events**

- **Oil & Gas Cybersecurity**  Houston, TX  Sep 17-21

**Private Training**

This course is also available through Private Training.

**Online Training**

- **OnDemand**
  Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
**DAY 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), and guide security teams to find threats in the environment. Today you 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 day features four hands-on labs that include building a Programmable Logic Controller (PLC), identifying information valuable about assets online through Shodan, completing an analysis of competing hypotheses, and ingesting threat intelligence reports. This will guide the practices of students during the rest of the labs in the course.

**Topics:**
- Case Study: Have:x, Introduction to ICS Active Defense and Incident Response
- Intelligence Life Cycle and Threat Intelligence
- ICS Information Attack Surface: External ICS Threat Intelligence
- Internal ICS Threat Intelligence: Sharing and Consuming ICS Threat Intelligence

**DAY 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, SGUIL, ELSA, CyberLens, Bro, NetworkMiner, 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: BlackEnergy2: ICS Asset and Network Visibility
- Identifying and Reducing the Threat Landscape
- ICS Network Security Monitoring – Collection
- ICS Network Security Monitoring – Detection
- ICS Network Security Monitoring – Analysis

**DAY 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 in an 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 students in this section 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: Stuxnet: Incident Response and Digital Forensics Overview
- Preparing an ICS Incident Response Team
- Evidence Acquisition
- Sources of Forensic Data in ICS Networks
- Time-Critical Analysis
- Maintaining and Restoring Operations

**DAY 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: German Steelworks: ICS Threat and Environment Manipulation Goals and Considerations
- Establishing a Safe Working Environment
- Analyzing Acquired Evidence
- Memory Forensics
- Malware Analysis Methodologies
- Case Study: BlackEnergy2 Automated Analysis
- Indicators of Compromise
- Environment Manipulation

**DAY 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
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center team leads and analysts
- ICS red team and penetration testers
- Active defenders

---

“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
Cyber Defense | 2-Day & Beta Courses

SEC402: The Secrets to Successful Cybersecurity Writing: Hack the Reader

Want to write better? Learn to hack the reader! Discover how to find an opening, break down your readers’ defenses, and capture their attention to deliver your message—even if they’re too busy or indifferent to others’ writing. This unique course, built exclusively for cybersecurity professionals, will strengthen your writing skills and boost your security career.

The course builds upon the author’s two decades of cybersecurity experience. You’ll learn from examples relevant to security professionals, whether they’re experts or beginners, managers or individual team members. The course focuses on common writing problems you’ll learn to avoid, instead of presenting tedious grammar rules or theoretical explanations. You’ll advance your writing by reviewing and improving real-world cybersecurity samples.

Master the writing secrets that’ll make you stand out in the eyes of your peers, colleagues, managers, and clients. Learn to communicate your insights, requests, and recommendations persuasively and professionally. Make your cybersecurity writing remarkable.

SEC440: Critical Security Controls: Planning, Implementing, and Auditing

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). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government and private organizations (including the NSA, DHS, GAO, and many others) that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and help find and mitigate damage from the attacks that get through.

SEC450: Blue Team Fundamentals: Security Operations and Analysis

SEC450 is designed to be an accelerated on-ramp for new cyber defense team members. Developed by an author with years of experience as a lead analyst and Security Operations Center manager, this course packs in all the essential explanations of tools, process, and data flow that every blue team member needs to know. Given the current shortage of cybersecurity professionals and a hiring gap that is only widening, organizations need a quick way to onboard new defenders. By providing a detailed explanation of the mission and mindset of a modern cyber defense operation, SEC450 squarely addresses that challenge by jumpstarting and empowering those on their way to becoming the next generation of blue teamers.

SEC455: SIEM Design & Implementation

Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization’s security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation. The use of professional services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations. A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEMs and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.
## Penetration Testing | 2-Day Courses

### SEC564: Red Team Operations and Threat Emulation

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world threats in order to train and measure the effectiveness of the people, processes, and technology used to defend environments. Built on the fundamentals of penetration testing, Red Teaming uses a comprehensive approach to gain insight into an organization’s overall security in order to test its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization’s security controls, hone its defensive capabilities, and measure the effectiveness of its security operations. The Red Team concept requires a different approach from a typical security test and relies heavily on well-defined TTPs, which are critical to successfully emulate a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve security is extremely valuable. Organizations spend a great deal of time and money on the security of their systems, and it is critical to have professionals who can effectively and efficiently operate those systems. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team engagements, and understand the role of a Red Team and its importance in security testing. This two-day course will explore Red Team concepts in-depth, provide the fundamentals of threat emulation, and help you reinforce your organization’s security posture.

<table>
<thead>
<tr>
<th>Live Training*</th>
<th>2 Day Course</th>
<th>12 CPEs</th>
<th>Laptop Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 15-16</td>
<td></td>
</tr>
<tr>
<td>CDI</td>
<td>Washington, DC</td>
<td>Dec 12-13</td>
<td></td>
</tr>
</tbody>
</table>

“The content from SEC564 is great and I will be able to implement it in my organization right away!”
-Kirk Hayes, Rapid 7

### SEC580: Metasploit Kung Fu for Enterprise Pen Testing

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws. The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

<table>
<thead>
<tr>
<th>Live Training*</th>
<th>2 Day Course</th>
<th>12 CPEs</th>
<th>Laptop Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security</td>
<td>Las Vegas, NV</td>
<td>Sep 15-16</td>
<td></td>
</tr>
<tr>
<td>CDI</td>
<td>Washington, DC</td>
<td>Dec 12-13</td>
<td></td>
</tr>
</tbody>
</table>

“SEC580 is a great course – right audience size, right pace, good labs, and excellent instruction.”
-Robert Lockwood, Fusion Cell Consulting
**IR & Forensics | Beta Course**

**FOR498: Battlefield Forensics & Data Acquisition**

The clock is ticking. You need to prioritize the most valuable evidence for processing. Let us show you how.

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 these data can live in many varied formats and locations. You must be able to first identify the data that you might need, determine where those data reside, and, finally, formulate a plan and procedures for collecting those 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, preserve, and respond to 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 forensic 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 identify, collect, preserve, and respond to data no matter where those data hide or reside.

**Live Training**

- **DFIRCON Miami**...... Coral Gables, FL...... Nov 4 - 9
- **Summit Events**
  - **DFIR**....................... Austin, TX............. Jul 27 - Aug 1

**6 Day Program | 36 CPEs | Laptop Required**

**Online Training**

- **OnDemand**
  - Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

---

**DevSecOps | 2-Day Courses**

**SEC534: Secure DevOps: A Practical Introduction**

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. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management (“Infrastructure as Code”), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance (“Compliance as Code”) and Continuous Monitoring. 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.

**2 Day Course | 12 CPEs | Laptop Required**

**Online Training**

- **Private Training**
  - This course is also available through Private Training.
MGT415: A Practical Introduction to Cyber Security Risk Management

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their workforce. As a result, people, not technology, have become the most common target for cyber attackers. The most effective way to secure the human element is to establish a mature security awareness program that goes beyond just compliance, changes people’s behaviors and ultimately creates a secure culture. This intense two-day course will teach you the key concepts and skills needed to do just that, and is designed for those establishing a new program or wanting to improve an existing one. The course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

Vulnerabilities are everywhere. There are new reports of problems within our systems and software every time we turn around. Directly related to this is an increase in the quantity and severity of successful attacks that seem to happen daily. Managing vulnerabilities in any size organization is challenging. Enterprise environments add scale and diversity that overwhelms many IT security and operation’s teams. Now 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, and security may seem unachievable.

The primary goal of this course is to equip those responsible for managing the infrastructure and application vulnerabilities within their organization with strategies and solutions that overcome the challenges and stumbling blocks they may encounter. In addition, the course provides participants a better understanding of how to manage vulnerabilities in the cloud and leverage new and exciting technologies and development patterns to increase the effectiveness of their program.

By understanding the problem and potential solutions, participants will be better prepared to meet this challenge and determine what might work for their organization. Through course discussions and other exercises participants will also be encouraged to share what is working and not working in their organizations.

Knowing that our environments are adopting cloud services and becoming more tightly integrated with them, we 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 performed on the final course day 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 this organization succeed.
HOSTED: **Assessing and Exploiting Control Systems**

This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, RF communications, Human Machine Interfaces (HMIs), and various forms of master servers and their ICS applications. Skills you will learn in this course will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building management, manufacturing, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors.

| 6 Day Course | 36 CPEs | Laptop Required |

**Live Training**

**Summit Events**

Oil & Gas Cybersecurity. Houston, TX .......... Sep 17-22

---

HOSTED: **Critical Infrastructure and Control System Cybersecurity**

This is an intermediate to advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. This course will provide hands-on analysis of control system environments allowing students to understand the environmental, operational and economic impacts of attacks like Stuxnet and supporting mitigating controls. The course features:

- A hands-on environment (PLC, HMI, Network Communications, Backtrack)
- Coverage of operational, cyber, and physical protective solutions
- Kits provided and used by pods of two attendees (Laptop, Customized I/O Trainer, PLC, HMI, communications infrastructure, CYBATIFIED Backtrack)

| 5 Day Course | 30 CPEs | Laptop Required |

---

HOSTED: **Physical Penetration Testing**

Those who attend this session will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Attendees will not only learn how to distinguish good locks and access control from poor ones, but will also become well-versed in picking and bypassing many of the most common locks used in North America in order to assess their own company’s security posture or to augment their career as a penetration tester.

| 2 Day Course | 12 CPEs | Laptop Not Needed |

**Live Training**

**Private Training**

This course is also available through Private Training.

---

HOSTED: **Physical Security Specialist – Full Comprehensive Edition**

This course is taught by the CORE Group, a firm with divisions that focus on penetration testing, physical defense, personal protection details, and law enforcement training. This training is ideal for anyone tasked with making physical security decisions for existing or new facilities. Students will be prepared to make educated and fiscally-responsible security decisions not only for their respective organizations but also for themselves. Participants will be able to approach any target, site-unseen, and then either conduct a walk-through assessment highlighting attack vectors, or proceed directly with an attack, gaining physical access to critical areas and infrastructure. Additionally, these newly-minted professionals will also be able to provide sound documentation while making recommendations to management or to their insurance providers, saving money for their companies.

| 6 Day Course | 36 CPEs | Laptop Required |

---

HOSTED: **Health Care Security Essentials**

This course is designed to provide attendees with an introduction to current and emerging issues in health care information security and regulatory compliance. The class provides a foundational set of skills and knowledge for students through the integration of case studies, hands-on labs, and defensible control considerations for securing and monitoring electronic protected health information (ePHI). Students will learn about actual attacks and incidents that have affected health care organizations and what can be done to mitigate the damage to prevent your organization from suffering a similar outcome.

| 2 Day Course | 12 CPEs | Laptop Required |
The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization's training needs.

As a SANS Voucher Program participant, you will be able to:

- Provide your cybersecurity team with the highest standard of skill training and certification available
- Give employees a simple way to select and procure the training they need, when they need it
- Easily approve and manage student enrollment
- Monitor employee training progress and exam scores to ensure satisfactory completion
- Track investments, debits, and account balance for optimal budgeting

Voucher Funds purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Voucher Funds must be used within 12 months, but the term can be extended with additional investments.

Get Started
Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little time as one week, your eligible team members can begin their training.

*Current exceptions from the SANS Voucher Program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.
Experience NetWars

Play solo or on a team of up to five players

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended.”
– Kyle McDaniel, Lenovo

Choose from:
- Core NetWars
- DFIR NetWars
- Cyber Defense NetWars
- ICS NetWars
- Grid NetWars

Develop skills in:
- Cyber Defense
- Penetration Testing
- Digital Forensics & Incident Response
- Industrial Control Systems & SCADA

Participation in NetWars is free for students taking 4-, 5-, or 6-day courses.
NetWars takes place in the evening, after class, and gives you an immediate opportunity to apply what you’ve learned in a fun, competitive, hands-on, and educational environment!
Seating is limited, so add NetWars when you register for your course.

www.sans.org/netwars
Advancing Cybersecurity Through Collaboration

“I was impressed by the expertise of the speakers and more impressed by the quality of attendees. Both the information presented in the conference and after-hours discussions were engaging and productive.”

- Doug Short, Trinity River Authority

Upcoming Summit & Training Events

Enterprise Defense  
Redondo Beach, CA | June 3-10

Security Operations  
New Orleans, LA | June 24 – July 1

DFIR  
Austin, TX | July 25 – Aug 1

Security Awareness  
San Diego, CA | Aug 5-14

Supply Chain Cybersecurity  
Washington, DC | Aug 12-19

Oil & Gas Cybersecurity  
Houston, TX | Sep 16-22

Threat Hunting & Incident Response  
New Orleans, LA | Sep 30 – Oct 7

SIEM  
Chicago, IL | Oct 7-14

Purple Team  
Dallas, TX | Oct 21-28

Cloud & DevOps Security  
Denver, CO | Nov 4-11

Pen Test HackFest  
Washington, DC | Nov 18-25
Join the **SANS.org community** today to enjoy these free resources at [www.sans.org/join](http://www.sans.org/join)

### Newsletters

**NewsBites**
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.

**OUCH!**
The world’s leading monthly, free security awareness newsletter designed for the common computer user.

### Webcasts

**Ask the Experts Webcasts**
SANS experts bring current and timely information on relevant topics in IT Security.

**Analyst Webcasts**
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

**WhatWorks Webcasts**
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

**Tool Talks**
Tool Talks are designed to give you a solid understanding of a problem and how a vendor’s commercial tool can be used to solve or mitigate that problem.

### Other Free Resources (SANS.org account is not necessary)

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

### Free Course Demos

With your **SANS.org account**, you can test drive many of our most popular courses. Simply click on “Free Course Demo” at the top of your selected course page on the website, and watch up to an hour of that course via the SANS OnDemand platform.

[www.sans.org/demos](http://www.sans.org/demos)

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.