THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS

DC Metro

JULY - DECEMBER 2016

HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

9 LOCATIONS

- CHANTILLY
- COLUMBIA
- VIRGINIA BEACH
- CRYSTAL CITY
- ARLINGTON
- BALTIMORE
- RICHMOND
- TYSONS CORNER
- WASHINGTON DC

39 COURSES ON

- CYBER DEFENSE
- DIGITAL FORENSICS
- PEN TESTING
- SECURITY MANAGEMENT
- APPLICATION SECURITY
- ICS SECURITY
- IT AUDIT
- CRITICAL SECURITY CONTROLS
- CYBER THREAT INTELLIGENCE

SAVE $400

by registering and paying early!

See page 49 for more details.

www.sans.org/dc-metro

GIAC-Approved Training

SANS DC Metro

July - December 2016

COMMUNITY SANS Chantilly
Chantilly, VA | Jul 25-30 | Sep 26-Oct 1 | Oct 24-28
www.sans.org/community

COMMUNITY SANS Columbia
Columbia, MD | Jul 18-23 | Aug 1- 6 | Aug 8-13
Aug 15-20 | Sep 12-17 | Sep 19-24 | Sep 26-Oct 1
www.sans.org/community

SANS Virginia Beach 2016
Virginia Beach, VA | Aug 22 - Sep 2
www.sans.org/virginia-beach

SANS NORTHERN VIRGINIA Crystal City 2016
Crystal City, VA | Sep 6-11
www.sans.org/crystal-city

SANS MENTOR – Arlington
Arlington, VA | Sep 13 - Nov 15
www.sans.org/mentor

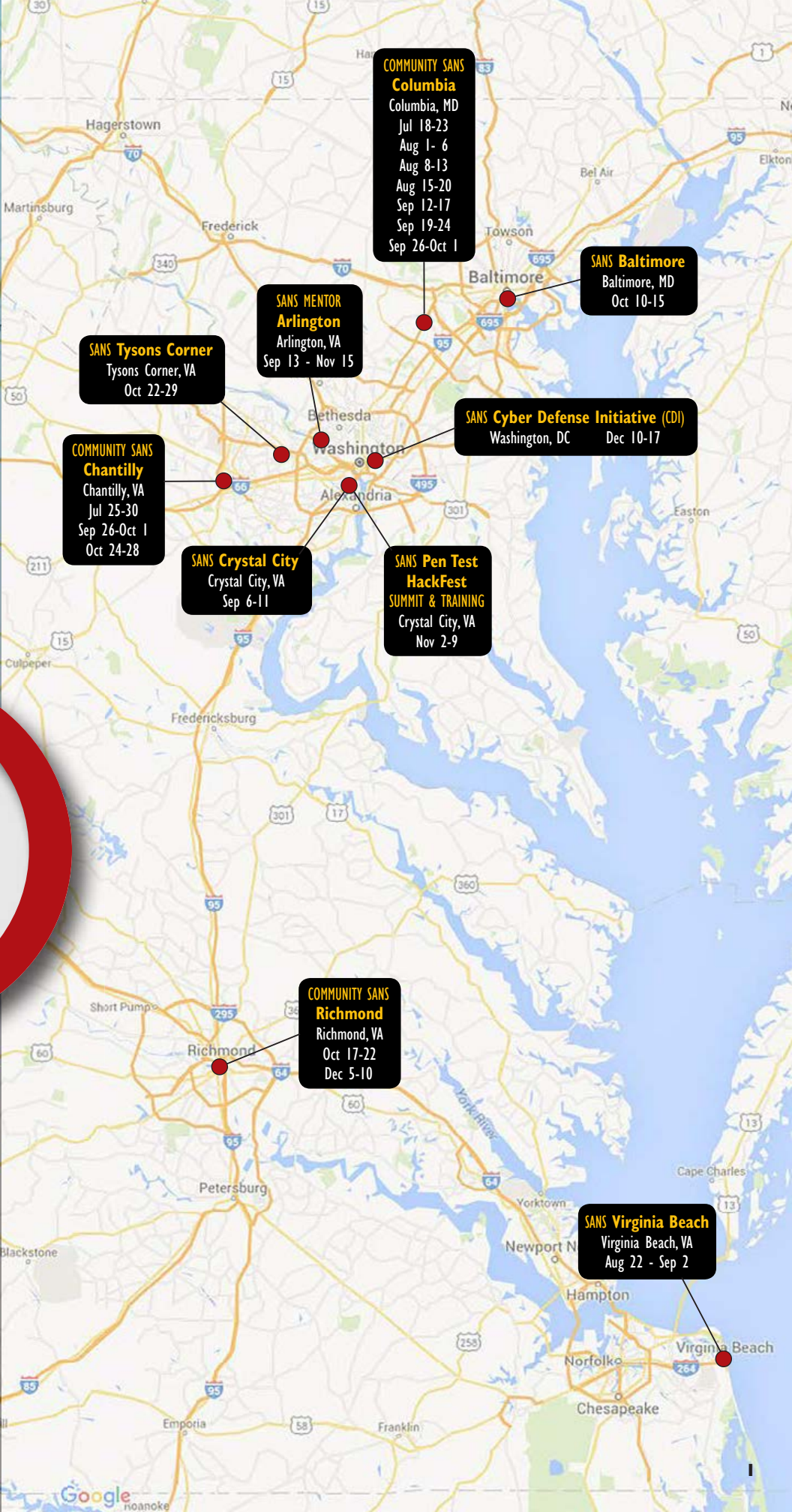
SANS Baltimore 2016
Baltimore, MD | Oct 10-15
www.sans.org/baltimore

COMMUNITY SANS Richmond
Richmond, VA | Oct 17 - 22 | Dec 5-10
www.sans.org/community

SANS Tysons Corner 2016
Tysons Corner, VA | Oct 22-29
www.sans.org/tysons-corner

SANS Pen Test HackFest SUMMIT & TRAINING
Crystal City, VA | Nov 2-9
www.sans.org/hackfest

SANS Cyber Defense Initiative (CDI) 2016
Washington, DC | Dec 10-17
www.sans.org/CDI


COMMUNITY SANS
Columbia
Columbia, MD
Jul 18-23
Aug 1- 6
Aug 8-13
Aug 15-20
Sep 12-17
Sep 19-24
Sep 26-Oct 1
SANS Baltimore
Baltimore, MD
Oct 10-15
SANS MENTOR
Arlington
Arlington, VA
Sep 13 - Nov 15
SANS Tysons Corner
Tysons Corner, VA
Oct 22-29
SANS Cyber Defense Initiative (CDI)
Washington, DC Dec 10-17
COMMUNITY SANS
Chantilly
Chantilly, VA
Jul 25-30
Sep 26-Oct 1
Oct 24-28
SANS Crystal City
Crystal City, VA
Sep 6-11
SANS Pen Test
HackFest
SUMMIT & TRAINING
Crystal City, VA
Nov 2-9
COMMUNITY SANS
Richmond
Richmond, VA
Oct 17-22
Dec 5-10
SANS Virginia Beach
Virginia Beach, VA
Aug 22 - Sep 2
Hagerstown
Martinsburg
Frederick
Bel Air
Towson
Baltimore
Bethesda
Washington
Alexandria
Easton
Culpeper
Fredericksburg
Short Pump
Richmond
Petersburg
Blackstone
York River
Yorktown
Newport N
Hampton
Cape Charles
Virginia Beach
Norfolk
Chesapeake
Emporia
Franklin
Roanoke
Google

SANS DC METRO

Course Schedule

For an up-to-date course list, please check the website:
www.sans.org/dc-metro

		Page No.		COMMUNITY SANS Chantilly Chantilly, VA Jul 25-Oct 28	COMMUNITY SANS Columbia Columbia, MD Jul 18-Oct 1	Virginia Beach Virginia Beach, VA Aug 22-Sep 2	Crystal City Crystal City, VA Sep 6-11	SANS MENTOR Arlington Arlington, VA Sep 13-Nov 15	Baltimore Baltimore, MD Oct 10-15	COMMUNITY SANS Richmond Richmond, VA Oct 17-Dec 10	Tysons Corner Tysons Corner, VA Oct 22-29	Pen Test HackFest SUMMIT & TRAINING Crystal City, VA Nov 2-9	Cyber Defense Initiative Washington, DC Dec 10-17
SEC301	Intro to Information Security	6		SEC301 Oct 24-28			SEC301						SEC301
SEC401	Security Essentials Bootcamp Style	7		SEC401 Sep 26-Oct 1	SEC401 Jul 18-23 Sep 12-17	SEC401	SEC401		SEC401	SEC401 Oct 17-22	SEC401		SEC401
SEC440	Critical Security Controls: Planning, Implementing, and Auditing	38									SEC440		SEC440
SEC501	Advanced Security Essentials – Enterprise Defender	8			SEC501 Sep 19-24	SEC501			SEC501		SEC501		SEC501
SEC503	Intrusion Detection In-Depth	9				SEC503							SEC503
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	10		SEC504 Jul 25-30	SEC504 Aug 8-13	SEC504	SEC504		SEC504	SEC504 Dec 5-10	SEC504	SEC504	SEC504
SEC505	Securing Windows and PowerShell Automation	11											SEC505
SEC511	Continuous Monitoring and Security Operations	12				SEC511							SEC511
SEC542	Web App Penetration Testing and Ethical Hacking	13					SEC542		SEC542			SEC542	SEC542
SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception	14									SEC550		SEC550
SEC560	Network Penetration Testing and Ethical Hacking	15			SEC560 Aug 1-6	SEC560			SEC560			SEC560	SEC560
SEC561	Immersive Hands-On Hacking Techniques	16				SEC561							SEC561
SEC562	CyberCity Hands-on Kinetic Cyber Range Exercise	17										SEC562	
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	18											SEC566
SEC567	Social Engineering for Penetration Testers NEW!	38											SEC567
SEC575	Mobile Device Security and Ethical Hacking NEW!	19				SEC575							SEC575
SEC579	Virtualization and Private Cloud Security	20											SEC579
SEC580	Metasploit Kung Fu for Enterprise Pen Testing	39											SEC580
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	21										SEC617	
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	22											SEC660
SEC760	Advanced Exploit Development for Penetration Testers	23										SEC760	SEC760
FOR408	Windows Forensic Analysis	24				FOR408	FOR408						FOR408
FOR508	Advanced Digital Forensics and Incident Response	25			FOR508 Sep 26-Oct 1	FOR508			FOR508		FOR508		FOR508
FOR518	Mac Forensic Analysis	26				FOR518							FOR518
FOR572	Advanced Network Forensics and Analysis	27			FOR572 Aug 15-20	FOR572							FOR572
FOR578	Cyber Threat Intelligence NEW!	28							FOR578				FOR578
FOR585	Advanced Smartphone Forensics	29				FOR585			FOR585				
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	30											FOR610
DEV522	Defending Web Applications Security Essentials	31											DEV522
MGT305	Technical Communication and Presentation Skills for Security Professionals	39											MGT305
MGT414	SANS Training Program for CISSP® Certification	32				MGT414		MGT414			MGT414		MGT414
MGT415	A Practical Introduction to Cyber Security Risk Management	40											MGT415
MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program	40									MGT433		MGT433
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	33				MGT512	MGT512				MGT512		MGT512
MGT514	IT Security Strategic Planning, Policy, and Leadership	34					MGT514		MGT514				MGT514
MGT535	Incident Response Team Management	40											MGT535
ICS456	Essentials for NERC Critical Infrastructure Protection NEW!	35											ICS456
ICS515	ICS Active Defense and Incident Response	36				ICS515			ICS515				ICS515
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	37									AUD507		AUD507
	CORE/DFIR NetWars Tournament	41				CORE						CORE	CORE/DFIR
	NetWars CyberCity	41										CyberCity	
	Pen Test HackFest Summit	43										Summit	

DC METRO INSTRUCTORS

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up-to-date and relevant to your job.

Doc Blackburn
SANS Instructor
SEC401: Chantilly

Mark Bristow
SANS Instructor
ICS515: Baltimore

Rebekah Brown
SANS Instructor
FOR578: Baltimore

Ovie Carroll
Certified Instructor
FOR408: CDI

Carlos Cajigas
SANS Instructor
FOR408: Virginia Beach

Dr. Eric Cole
Faculty Fellow
SEC401: Virginia Beach
SEC401: Tysons Corner

Eric Conrad
Senior Instructor
SEC511: Virginia Beach
SEC542: CDI

Tim Conway
SANS Instructor
ICS456: CDI

David Cowen
Certified Instructor
FOR408: Crystal City

Christopher Crowley
Certified Instructor
SEC575: Virginia Beach
SEC575: CDI
MGT535: CDI

Adrien de Beaupre
Certified Instructor
SEC542: Crystal City
SEC542: Pen Test HackFest
SEC560: Virginia Beach

Jason Dely
SANS Instructor
ICS515: Virginia Beach

Sarah Edwards
Certified Instructor
FOR518: Virginia Beach
FOR518: CDI

Mark Elliott
SANS Instructor
SEC501: Columbia

Steven Elovitz
SANS Instructor
MGT414: Arlington

Kevin Fiscus
Certified Instructor
SEC503: Virginia Beach
SEC504: Baltimore
SEC561: Virginia Beach
SEC561: CDI

Jason Fossen
Faculty Fellow
SEC505: CDI

Bryce Galbraith
Principal Instructor
SEC550: CDI
SEC580: CDI

Tim Garcia
SANS Instructor
SEC401: Crystal City

Philip Hagen
Certified Instructor
FOR572: Virginia Beach
FOR572: Columbia
FOR572: CDI

Ron Hamann
SANS Instructor
SEC401: Columbia

G. Mark Hardy
Certified Instructor
MGT512: Virginia Beach
MGT512: Tysons Corner

Paul A. Henry
Senior Instructor
SEC501: Baltimore
SEC501: Tysons Corner
SEC501: CDI

Moses Hernandez
SANS Instructor
SEC560: Columbia

David Hoelzer
Faculty Fellow
MGT512: Crystal City

Micah Hoffman
Certified Instructor
SEC542: Baltimore

Frank Kim
Certified Instructor
MGT514: CDI

Rob Lee
Faculty Fellow
FOR508: Virginia Beach

Robert M. Lee
Certified Instructor
FOR578: Baltimore
ICS515: Virginia Beach
ICS515: CDI

James Lyne
Certified Instructor
SEC660: CDI

Heather Mahalik
Senior Instructor
FOR585: Baltimore

Randy Marchany
Certified Instructor
SEC440: Tysons Corner
SEC440: CDI

David Mashburn
SANS Instructor
SEC504: Chantilly

Jeff McJunkin
SANS Instructor
SEC560: Baltimore

Tim Medin
Certified Instructor
SEC562: Pen Test HackFest

David R. Miller
Certified Instructor
MGT414: Tysons Corner
MGT414: CDI

Seth Misenar
Senior Instructor
SEC511: CDI
MGT414: Virginia Beach

Cindy Murphy
Certified Instructor
FOR585: Virginia Beach

Michael Murr
Principal Instructor
SEC504: Virginia Beach
SEC560: CDI

My-Ngoc Nguyen
Certified Instructor
SEC301: Crystal City

Stephen Northcutt
Faculty Fellow
MGT512: CDI

Jorge Orchilies
SANS Instructor
SEC504: Columbia

Keith Palmgren
Senior Instructor
SEC301: CDI

Larry Pesce
Certified Instructor
SEC617: Pen Test HackFest

Mike Pilkington
Certified Instructor
FOR508: Columbia

Chris Pizor
Certified Instructor
SEC504: Pen Test HackFest
SEC550: Tysons Corner

Hal Pomeranz
Faculty Fellow
FOR508: Baltimore

Mike Poor
Senior Instructor
SEC503: CDI

Clay Risenhoover
Certified Instructor
AUD507: Tysons Corner
AUD507: CDI

Dave Shackleford
Senior Instructor
SEC567: CDI
SEC579: CDI

Bryan Simon
Certified Instructor
SEC401: Baltimore
SEC401: CDI
SEC501: Virginia Beach
MGT305: CDI

Stephen Sims
Senior Instructor
SEC760: CDI

Ed Skoudis
Faculty Fellow
SEC560: Pen Test HackFest

Lance Spitzner
Certified Instructor
MGT433: Tysons Corner
MGT433: CDI

John Strand
Senior Instructor
SEC504: CDI

James Tarala
Senior Instructor
SEC566: CDI
MGT415: CDI

Chad Tilbury
Senior Instructor
FOR408: Virginia Beach
FOR508: CDI

Alissa Torres
Certified Instructor
SEC504: Crystal City
FOR508: Tysons Corner

Johannes Ullrich, PhD
Senior Instructor
DEV522: CDI

Jake Williams
Certified Instructor
SEC760: Pen Test HackFest
FOR578: CDI

Mark Williams
SANS Instructor
MGT514: Crystal City
MGT514: Baltimore

Lenny Zeltser
Senior Instructor
FOR610: CDI

Eric Zimmerman
SANS Instructor
FOR508: Baltimore

SANS SEC301

Intro to Information Security

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

Crystal City
Sep 6-10 • Nguyen

Chantilly
Oct 24-28 • Staff

CDI
Dec 12-16 • Palmgren

www.giac.org/gisf

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"SEC301 is the perfect blend of technical and practical information for someone new to the field, would recommend to a friend!"

-Steve Mecco, Draper

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

- Are you new to information security 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 information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Intro to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have no prior knowledge of security and limited knowledge of technology. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec 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 course up the line, **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.***

Author Statement

If you want to be good at something, whether it be sports, music, science, math, or information security, you MUST have a solid grasp of the fundamentals. In fact, the better you understand the fundamentals the better you will be at a particular skillset. Without that foundation to build on, it is almost impossible to become a master at something. The Introduction to Information Security course is all about building those fundamentals and creating that foundation. One of the things I enjoy most is seeing a student have that "ah-ha" moment. The moment when they suddenly understand a topic for the first time – often a topic they have wondered about for years. You can almost literally see the "light-bulb" of understanding appear over their head. There are "ah-ha" moments at every turn and on every day of this course.
-Keith Palmgren

Security Essentials Bootcamp Style

SANS SEC401

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.

Who Should Attend

- Security professionals
- Managers
- Operations personnel
- IT engineers and supervisors
- Administrators
- Forensic specialists, penetration testers, and auditors
- Anyone new to information security with some background in information systems and networking

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, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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.

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 28 - Sep 2 • Cole

Crystal City
Sep 6-11 • Garcia

Columbia
Jul 18-23 • Hamann
Sep 12-17 • Staff

Chantilly
Sep 26-Oct 1 • Blackburn

Baltimore
Oct 10-15 • Simon

Richmond
Oct 17-22 • Staff

Tysons Corner
Oct 24-29 • Cole

CDI
Dec 12-17 • Simon

"This training was more than I expected. I never thought I would learn so much in such a short amount of time."
-Jote Aga,
Dept. of Veterans Affairs

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian


www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

SANS SEC501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 22-27 • Simon

Columbia
Sep 19-24 • Elliott

Baltimore
Oct 10-15 • Henry

Tysons Corner
Oct 24-29 • Henry

CDI
Dec 12-17 • Henry

www.giac.org/gced

www.sans.edu

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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.

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

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.

"Really, really good info and hands on, and lots of both!"
-Danielle Perchert, Sandia National Laboratories

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.

"SEC501 is the perfect course to immerse enterprise security staff into essential skills. Failing to attend this course is done at the peril of your organization." -John N. Johnson, Houston Police Department

Author Statement

After one recent class, a student ran up and gave me a big hug (he was a retired football player, so I did not argue) and said, "SANS is awesome. I have been frustrated in my job for over a year and had lost hope that you really could secure an organization and that anything I did made a difference. Just as my light of hope was burning out, I decided to take the Security Essentials course, figuring it was a lost cause. After this class the fire is burning brighter than it ever was. I feel like a kid again and cannot wait to go back to my company and make a difference. However, I think my boss is scared because I called him eight times throughout the week, telling him all of the great information and practical knowledge I learned!"

Having taught thousands of students, I am confident you will be just as excited and get similar results from SEC501. However, just for reference, hugs are optional.

-Dr. Eric Cole

Intrusion Detection In-Depth

SANS SEC503

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?

SEC503: Intrusion Detection In-Depth 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 HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. 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. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

"Today has been brilliant, bringing all of our skills together to achieve the challenge. I wish we could do this every day!"
-Hayley Roberts, MOD

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops 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.

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 often 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. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

"SEC503 covers the best processes for intrusion analysis and how to cut out most of the network noise and identify the important traffic."
-Mike Boya, Warner Bros.

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 28 - Sep 2 • Fiscus

CDI
Dec 12-17 • Poor

GCIA
www.giac.org/gcia

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

Who Should Attend

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

SANS SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
37 CPEs
Laptop Required

TRAINING EVENTS

Chantilly
Jul 25-30 • Mashburn

Columbia
Aug 8-13 • Orchilles

Virginia Beach
Aug 28 - Sep 2 • Murr

Crystal City
Sep 6-11 • Torres

Baltimore
Oct 10-15 • Fiscus

Tysons Corner
Oct 24-29 • Staff

Pen Test HackFest
Nov 4-9 • Pizor

Richmond
Dec 5-10 • Staff

CDI
Dec 12-17 • Strand

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or 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.

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"Our organization has incident response pieces all over. This course is valuable in putting the pieces together and improving the plan and, more importantly, the mindset." -Tyler Burwitz, TEEX

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. It 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.

Author Statement

One of my greatest joys in life is helping people understand the complex landscape of security so that they can implement really effective defenses. It may be difficult to fully grasp what truly impacts the security of your organization versus what is simply product marketing hype. This class is the nexus between attacks and defenses, chock full of vital information for thwarting today's nastiest attacks. Ed Skoudis and I continuously refine this class on the basis of the many penetration tests we conduct and the incidents we handle regularly. We strive to keep the material relevant, interesting, and directly applicable to the job of infosec professionals. And I personally live for the moments when the light goes on within a 504 student and they finally see through the noise and begin to understand what is important from a threat and vulnerability perspective. -John Strand

Securing Windows and PowerShell Automation

SANS SEC505

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – *now what?* A major theme of this course is defensible design: 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 Security Information and Event Manager (SIEM) or monitoring system tells you a Domain Admin account has been compromised, *IT'S TOO LATE.*

For the assume breach mindset, we must carefully delegate *limited* administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

"SEC505 is very well structured and organized and provided me with an in-depth understanding of Windows security." -Rochana Lahiri, BCBSLA

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.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

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 SecOps/DevOps, it can save money, too. Besides, PowerShell is also simply fun to use.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate those Windows-related Critical Security Controls that are the most effective, but also the most difficult to implement, especially in large environments.

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 agile Windows security at the same time!

"I loved SEC505 and when I return to the office, I am recommending it to the rest of my team."
-Alex Fox, Federal Home Loan Bank Chicago

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

CDI
Dec 12-17 • Fossen

www.giac.org/gcwn

www.sans.edu

www.sans.org/cyber-guardian


www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Security Operations engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure or smart cards
- Anyone who needs to reduce malware infections

SANS SEC511

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 22-27 • Conrad

CDI
Dec 12-17 • Misenar

www.giac.org/gmon

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"I run SOCs and this course provides a gut check against what we are doing today."

-Tim Housman,
General Dynamics IT

Who Should Attend

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

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant 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.

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

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

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 (Day 6) 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. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Web App Penetration Testing and Ethical Hacking

SANS SEC542

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. 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.

Students will come to understand major web application flaws and their exploitation and, most importantly, 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. The 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 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 to hammer home lessons learned.

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Crystal City
Sep 6-11 • de Beaupre

Baltimore
Oct 10-15 • Hoffman

Pen Test HackFest
Nov 4-9 • de Beaupre

CDI
Dec 12-17 • Conrad

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"The content in SEC542 is very relevant as it features recently discovered vulnerabilities."
-Malcolm King, Morgan Stanley

Who Should Attend

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

SANS SEC550

Active Defense, Offensive Countermeasures & Cyber Deception

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

Tysons Corner
Oct 24-28 • Pizor

CDI
Dec 12-16 • Galbraith

"SEC550 is the next step in the evolution of cyber defense – learning to make the hacker's job harder, track their movement, and get attribution."

-Mick Leach, Nationwide

Who Should Attend

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

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools that will be at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

What You Will Receive

- A fully functioning Active Defense Harbinger Distribution ready to deploy
- Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments

Author Statement

I wrote this course to finally make defense fun, to finally throw some confusion at the attackers, and to change the way we all look at defense. One of the most frequent questions I get is why offensive countermeasures are so important. Many people tell me that we cannot ignore patching, firewalls, policies, and other security management techniques. I cannot agree more. The techniques presented in this course are intended for organizations that have gone through the process of doing things correctly and want to go further. Get your house in order, and then play. Of course, there will be challenges for anyone trying to implement offensive countermeasures in their organization. However, they can all be faced and overcome.

-John Strand

Network Penetration Testing and Ethical Hacking

SANS SEC560

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 masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, 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 knowledge you've mastered in this course.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

You will 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.

"I learned more in one class then in years of self study!"
-Bradley Milhorn, Compucom Inc.

Six-Day Program
37 CPEs
Laptop Required

TRAINING EVENTS

Columbia
Aug 1-6 • Hernandez

Virginia Beach
Aug 22-27 • de Beaupre

Baltimore
Oct 10-15 • McJunkin

Pen Test HackFest
Nov 4-9 • Skoudis

CDI
Dec 12-17 • Murr

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

SANS SEC561

Immersive Hands-On Hacking Techniques

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 22-27 • Fiscus

CDI
Dec 12-17 • Fiscus

"Hands down, one of the best SANS courses I have taken. We learned cutting-edge pen testing techniques in a hands-on environment that challenged my abilities and increased my overall knowledge."

-Dave Odom, Bechtel

Who Should Attend

- Security professionals
- Systems and network administrators
- Incident response analysts
- Forensic analysts
- Penetration testers
- Red and blue team members

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered **SEC561: Immersive Hands-On Hacking Techniques** from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time during in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

Topics addressed in the course include:

- Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation.
- Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks.
- Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools.
- Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access.
- Scouring through web applications and mobile systems to identify and exploit devastating developer flaws.
- Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques.
- Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization's exposure to one of the most damaging attack vectors widely used today.

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand-new and custom-developed scenarios built just for this course on the innovative **NetWars** challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Author Statement

In creating this course, we focused on getting as much practical, hands-on skill building into the classroom as possible. Each day begins with a short briefing on the technical topics students will work on throughout the day. Then, students build their skills analyzing real-world target systems in the classroom. When students walk out of the class, they will have mastered over 100 new techniques for finding, exploiting and then fixing security flaws. Just as aircraft pilots need more 'stick' time learning how to fly, this course provides penetration testers and other security professionals with the real-world experience they need to excel in their work. -Josh Wright

CyberCity Hands-on Kinetic Cyber Range Exercise

SANS SEC562

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Pen Test HackFest
Nov 4-9 • Medin

Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend this important infrastructure. In this innovative and cutting-edge course based on the SANS CyberCity kinetic range, you will learn how to analyze and assess the security of control systems and related infrastructure, finding vulnerabilities that could result in significant kinetic impact.

NetWars CyberCity

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and InfoSec pros that cyber action can have significant kinetic impact in the physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, the military, government, and commercial organizations have an increasing need for skilled defenders to protect critical infrastructure. We engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructure. CyberCity engages participants to defend the city's components from terrorist cyber attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

Participants engage in missions, with specific operation orders describing the defensive or offensive goal they need to achieve. On some missions, participants prevent attackers from undermining the CyberCity infrastructure and wreaking havoc, with all the kinetic action captured through streaming video cameras mounted around the physical city. On offensive missions, participants must seize control of CyberCity assets, retaking them from adversaries and using them to achieve a kinetic impact specified in their operation orders. Each mission includes not only a list of goals to be achieved, but also specific sensitive city assets that are out of bounds for the engagement, requiring additional tactical planning to adhere to the rules of engagement.

To achieve mission objectives, participants work as a team, engaging in effective mission planning, devising overall strategies and particular tactics, and exercising detailed technical skills. Furthermore, some participants will be charged as leaders of their teams, helping to build and assess leadership skills, decision-making capabilities, and the ability to brief senior leadership. Multiple realistic defensive and offensive missions test the cyberspace engineers' ability to thwart the best efforts of a well-funded terrorist organization or other cyber attacker trying to control city assets.

The main objectives of CyberCity are to:

- Teach cyber warriors and their leaders the potential kinetic impact of cyber attacks
- Provide a hands-on, realistic kinetic cyber range with engaging missions to conduct defensive and offensive actions
- Develop capabilities for defending and controlling critical infrastructure components to mitigate or respond to cyber attacks
- Demonstrate to senior leaders and planners the potential impact of cyber attacks and cyber warfare

"Very, very, very excellent course! I would like to take this course again."

-Masashi Fujiwara, Hitachi Ltd

Who Should Attend

- Red and blue team members
- Cyber warriors
- Incident handlers
- Penetration testers
- Ethical hackers
- Other security personnel who are first responders when systems come under attack

SANS SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

CDI
Dec 12-16 • Tarala

www.giac.org/gccc

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or 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

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 on how to implement 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.

"I'm leaving the class with a great mindset aimed at evaluating the current environment and controls. SEC566 was good information with a great instructor!" -Tom Kozelsky, Nexeo Solutions

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 defence."

SANS' 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.

Mobile Device Security and Ethical Hacking

SANS SEC575

NEW!

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 22-27 • Crowley

CDI
Dec 12-17 • Crowley

www.giac.org/gmob

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

Imagine an attack surface spread throughout 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. You don't need to imagine any further because this 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.**

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.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in **Apple iOS**, **Android**, and wearable devices including **Apple Watch** and **Android Wear**. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation 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 devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

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 the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including **Mobile App Report Cards** to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. 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 in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. 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 being 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.**

"Taking this course was a great opportunity to ask an expert all my questions, good broad overview and mobile threats background!"
-Tom G., GovCert UK

Who Should Attend

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

SANS SEC579

Virtualization and Private Cloud Security

Six-Day Program
36 CPEs
LAPTOP PROVIDED

TRAINING EVENTS

CDI
Dec 12-17 • Shackleford

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

One of today's most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. There are even security benefits of virtualization: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

"SEC579 was one of the best-produced SANS courses I have taken. The blend of operations and security was extremely valuable." -Scott Towery, Visions

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls.

"Great course! Anyone involved with managing virtual system environments will benefit from taking SEC579." -Randall R., Defense Security Services

In addition, many organizations are evolving virtualized infrastructure into private clouds, internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

"Dave is an excellent teacher and communicator. He made a highly technical course interesting and the overall experience was thoroughly enjoyable!" -Wayne Rosen, Adnet Systems, Inc.

Who Should Attend

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

Author Statement

Seeing the growth in virtualization technology over the past decade, I realized how important it was to educate security professionals on how the nature of their infrastructure is changing. We cannot keep securing systems the same way when the footprint of our data centers is radically different! As more organizations build private and hybrid clouds, we are changing trust models toward shared infrastructure as well. This course will help security, IT operations and audit team members develop a solid understanding of what is changing and how they can best secure these new technologies.

-Dave Shackleford

Wireless Ethical Hacking, Penetration Testing, and Defenses

SANS SEC617

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT

Pen Test HackFest
Nov 4-9 • Pesce

www.giac.org/gawn

www.sans.edu

www.sans.org/cyber-guardian

Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, it is growing in deployment and utilization with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies like ZigBee and Z-Wave offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, Bluetooth Low Energy, and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

"The detailed cryptographic explanations made it easier to understand how various encryption algorithms work." -Jonathan Wilhoit, Fluor

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. **This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker.** Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. You'll also develop attack techniques leveraging Windows 7 and Mac OS X. We'll examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the **SWAT Toolkit**, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

"I will use this knowledge to apply the best possible security to wireless guest networks where access is mandated to be easy." -Juan Reynoso, Fox

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

Author Statement

With the tremendous success of WiFi, other wireless protocols have also emerged to satisfy the needs of longer-distance wireless systems (WiMAX), lightweight embedded device connectivity (ZigBee and IEEE 802.15.4), and specialty interference-resilient connectivity (Bluetooth and DECT). Today, it's not enough to be a WiFi expert; you also need to be able to evaluate the threat of other standards-based and proprietary wireless technologies as well. In putting this class together, I wanted to help organizations recognize the multi-faceted wireless threat landscape and evaluate their exposure through ethical hacking techniques. Moreover, I wanted my students to learn critical security analysis skills so that, while we focus on evaluating wireless systems, the vulnerabilities and attacks we leverage to exploit these systems can be applied to future technologies as well. In this manner, the skills you build in this class remain valuable for today's wireless technology, tomorrow's technology advancements, and for other complex systems you have to evaluate in the future as well. -Joshua Wright

"If you're thinking about wireless take this course. If you're not, take this course."
-Greg Notch, NHL

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

SANS SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENT

CDI
Dec 12-17 • Lyne

www.giac.org/gxpn

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"The SEC660 course was hands-on, packed with content, and current to today's technology!"

-Michael Horken, Rockwell Automation

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.**

Advanced Exploit Development for Penetration Testers

SANS SEC760

Six-Day Program
46 CPEs
Laptop Required

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 skillset 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 skillset regardless of the increased complexity. **SEC760: Advanced Exploit Development for Penetration Testers** 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.

"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

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
- The importance of utilizing 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

"As always, I think SANS training is extremely valuable for any security professional. This course sits on top of the mountain of great SANS material." -Doug Rodgers, Wells Fargo

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 7/8/10, 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

TRAINING EVENTS

Pen Test HackFest
Nov 4-9 • Jake Williams

CDI
Dec 12-17 • Sims

Bundle OnDemand
with this course
www.sans.org/ondemand

Not sure if you are ready for SEC760?

Take this 10 question quiz:
www.sans.org/sec760/quiz

Who Should Attend

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

SANS FOR408

Windows Forensic Analysis

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 22-27 • Cajigas, Tilbury

Crystal City
Sep 6-11 • Cowen

CDI
Dec 12-17 • Carroll

www.giac.org/gcfe

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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

Who Should Attend

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

All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key 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 masters capable of piecing together what happened on computer systems second by second.

"I have been doing forensic investigations for several years, but would highly recommend this course (FOR408) for both new and old forensic investigations." -Robert Galarza, JP Morgan Chase

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll 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 unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR408 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook details the tools and techniques that each investigator should follow to solve a forensic case.

Advanced Digital Forensics and Incident Response

SANS FOR508

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occurred
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An advanced persistent threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Who Should Attend

- System administrators
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- Security Operations Center (SOC) personnel and information security practitioners
- SANS FOR408 and SEC504 graduates

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

"FOR508 has been the best DFIR course I've taken so far. All the material is recent and it shows a lot of time went into the material."
-Louise Cheung, Stroz Friedberg

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

"So far this is the best course I've taken in 20 years."
-Mauricio Bellido Jr., USG

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

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

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 28 - Sep 2 • Lee

Columbia
Sep 26-Oct 1 • Pilkington

Baltimore
Oct 10-15
Pomeranz, Zimmerman

Tysons Corner
Oct 24-29 • Torres

CDI
Dec 12-17 • Tilbury

GCFA
www.giac.org/gcfa

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

SANS
FOR518

Mac Forensic Analysis

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 28 - Sep 2 • Edwards

CDI
Dec 12-17 • Edwards

▶II **BUNDLE ONDEMAND**
WITH THIS COURSE
www.sans.org/ondemand

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, or 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/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 FOR408, FOR508, FOR526, FOR610, FOR585 alumni looking to round out their forensic skills

Digital forensic 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, yet most investigators are familiar with Windows-only machines.

"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."
-Naveel Koya, AC-DAC – Trivandrum

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.

FOR518: Mac Forensic Analysis will teach you:

- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) 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 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.
- **Mac Technologies:** How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

"Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."
-Kevin J. Ripa, Computer Evidence Recovery, Inc.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

FORENSICATE DIFFERENTLY!

"Very comprehensive in-depth coverage of the course topic. Excellent reference materials as a takeaway."
-Jennifer Barnes, Indiana State Police

Advanced Network Forensics and Analysis

SANS FOR572

The network itself IS the new investigative baseline.

There is simply no incident response action that doesn't include a communications component any more. Whether you conduct threat hunting operations, traditional casework, or post-mortem incident response, understanding the nature of how systems have communicated is critical to success. Even in disk- and memory-based incident response work, artifacts that clarify a subject's network actions can be keystone findings you can't afford to miss. Whether you are handling a data breach, intrusion scenario, or employee misuse case, or threat hunting (proactively trawling your organization's data stores for evidence of an undiscovered compromise), the need to effectively examine and interpret network artifacts is here to stay.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge and analytic approach needed to incorporate a network perspective into proactive hunting or traditional casework. Even the most skilled attacker can't fully escape leaving some evidence of communications on the network, so you'll learn the skills to identify reconnaissance, exploitation, operational, command-and-control, and data exfiltration phases of an incident. If you're chasing leads on an existing case or seeking evidence of a compromise you haven't yet discovered, the network is the key to success. 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 exploration, 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 already under way.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cyber crime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpxtract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy to make easy work of ripping through hundreds and thousands of data records.

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Columbia
Aug 15-20 • Hagen

Virginia Beach
Aug 28 - Sep 2 • Hagen

CDI
Dec 12-17 • Hagen

www.giac.org/gnfa

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Incident response team members and forensicators
- 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

SANS
FOR578

Cyber Threat Intelligence

NEW!

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

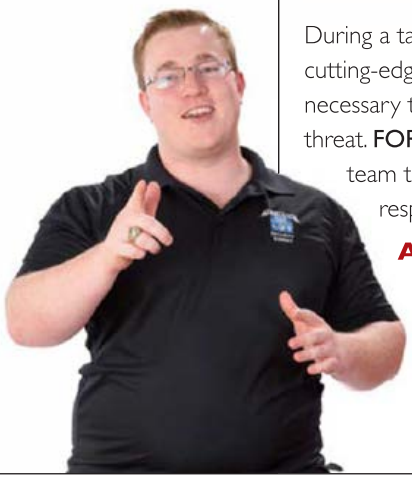
Baltimore
Oct 10-14 • M. Lee & Brown

CDI
Dec 12-16 • J. Williams

THERE IS NO TEACHER BUT THE ENEMY!

Who Should Attend

- Incident response team members
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level



Make no mistake: current computer network defense and incident response contain a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions.

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as **cyber threat intelligence** – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. **FOR578: Cyber Threat Intelligence** will train you and your team to determine, scope, and select resilient courses of action in response to such intrusions and data breaches.

Author Statement

When considering the value of threat intelligence, most individuals and organizations ask themselves three questions: What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community. -Robert M. Lee

Advanced Smartphone Forensics

SANS FOR585

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 22-27 • Murphy

Baltimore
Oct 10-15 • Mahalik

www.giac.org/gasf

www.sans.edu

▶II
BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, 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: Advanced Smartphone Forensics** will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data are saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting 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 class exceeded my expectations. The material is cutting edge!"
-Kevin McNamara, San Diego Police Dept.

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools 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.

"It's real-world practical info. Not just textbook!"
-Reza Salari, DRS Technologies

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you're working on the day you finish the course.

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 texts and apps can and will be used against them!

SMARTPHONE DATA CAN'T HIDE FOREVER –
IT'S TIME TO OUTSMART THE MOBILE DEVICE!

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- IT auditors
- SANS SEC575, FOR408, FOR518, and FOR508 graduates looking to take their skills to the next level

SANS FOR610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT

CDI
Dec 12-17 • Zeltser

www.giac.org/grem

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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 prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to understand the inner workings of malicious software and uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. Additionally, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

"This is a highly valuable course that equips one with the necessary skill to start on malware reverse engineering." -Kelvin Heng, DSTA

This course will teach you how to handle self-defending malware. You'll learn how to bypass the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts and deobfuscating JavaScript and VBScript to understand the nature of the attack.

You will also learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if it exhibits rootkit characteristics.

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 malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. 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.

Defending Web Applications Security Essentials

SANS DEV522

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENT

CDI
Dec 12-17 • Ullrich

www.giac.org/gweb

SANS Technology Institute

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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.

"The current security landscape is rapidly changing and the course content is relevant and important to software security and compliance software." -Scott Hoof, Tripwire, Inc.

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.

"As a developer, I felt that this training gave me better understanding on what I can do to make my applications more secure and understand the vulnerabilities that exist."
-Lerma Winchell, Vystar Credit Union

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 PCI requirements

SANS MGT414

SANS Training Program for CISSP® Certification

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 28 - Sep 2 • Misenar

Arlington
Sep 13 - Nov 15 • Elovitz

Tysons Corner
Oct 24-29 • Miller

CDI
Dec 12-17 • Miller

www.giac.org/gisp

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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 network 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

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2016 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

"I think the course material and the instructor are very relevant for the task of getting a CISSP. The overall academic exercise is solid."

-Aaron Lewter, Availity

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.

Obtaining Your CISSP® Certification Consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of your résumé
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Periodic audit of CPEs to maintain the credential

"This is a great way to refresh and review my knowledge before sitting for the CISSP exam. This course not only focused on the material at hand, but portrayed it with real-life examples that made it easy to relate to! One of the best classes and experiences I have had."

-Glenn C., Leidos

Take advantage of SANS' CISSP® Get Certified Program currently being offered.

www.sans.org/cissp

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS MGT512

This completely updated course is designed to empower advancing managers who want to 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. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!"
-John Madick, Epiq Systems, Inc.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression,™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

"MGT512 has great info for newly assigned managers to cybersecurity."
-Kerry T., U.S. Army Corps of Engineers

Five-Day Program
33 CPEs
Laptop NOT Needed

TRAINING EVENTS

Virginia Beach
Aug 22-26 • Hardy

Crystal City
Sep 6-10 • Hoelzer

Tysons Corner
Oct 24-28 • Hardy

CDI
Dec 12-16 • Northcutt

www.giac.org/gslc

www.sans.edu


www.sans.org/8140


Bundle OnDemand
with this course
www.sans.org/ondemand

Who Should Attend

- All newly appointed information security officers
- Technically-skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what their technical people are telling them

SANS MGT514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
30 CPEs
Laptop NOT Needed

TRAINING EVENTS

Crystal City
Sep 6-10 • M. Williams

Baltimore
Oct 10-14 • M. Williams

CDI
Dec 12-16 • Kim

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This is a great foundational course as we realize the importance of bringing a business perspective to security."
-Nairobi Kim, Wells Fargo

Who Should Attend

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

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 teaches security professionals how to do three things:

Develop Strategic Plans

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn 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 develop and assess policy to successfully guide your organization.

Develop Management and Leadership Skills

Leadership is a capability 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 while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to 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 work effectively with your business partners.

Essentials for NERC Critical Infrastructure Protection

SANS ICS456

NEW!

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENT

CDI
Dec 12-16 • Conway

ICS456: Essentials for NERC Critical Infrastructure Protection is a five-day course that 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), the North American Electric Reliability Corporation (NERC), and the regional entities. It provides multiple approaches to identifying and categorizing BES Cyber Systems and helps asset owners determine the specific implementations applicable to the requirements. Additionally, the course covers implementation strategies for the Version 5/6 standards with a balanced practitioner approach to both cybersecurity benefits and regulatory compliance. The course sections are as follows:

ICS456.1: Asset Identification and Governance. A transition is under way from NERC Critical Infrastructure Protection (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 one, students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP standards fit into the overall framework of the reliability standards.

ICS456.2: Access Control and Monitoring. Strong physical and cyber access controls are at the heart of any good cybersecurity program. On day two we move beyond the "what" of CIP compliance to understanding the "why" and the "how."

ICS456.3: 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 three, students will dive into CIP-007.

ICS456.4: Information Protection and Response. Education is key to every organization's success with NERC CIP. After this session on information protection and response, ICS456 students will be knowledgeable advocates for CIP when they return to their place of work.

ICS456.5: CIP Process. On the final day students will learn the key components for running an effective CIP compliance program. Topics will include CIP processes for maintaining compliance, preparing for an audit and following up on it, CIP industry activities, standards process, and the CIP of the future.

"SANS course work is the most thorough learning available anywhere. What you learn is not only conceptual, but it also is hands-on showing you what you do, why you do it, and how you can apply what you learn to real-world solutions to problems."

-Duane Tucker, Baymark Partners

Who Should Attend

- IT and OT (ICS) cybersecurity personnel
- Field support personnel
- Security operations personnel
- Incident response personnel
- Compliance staff
- Team leaders
- Governance officials
- Vendors/Integrators
- Auditors

SANS
ICS515

ICS Active Defense and Incident Response

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

Virginia Beach
Aug 29-Sep 2 • M. Lee, Dely

Baltimore
Oct 10-14 • Bristow

CDI
Dec 12-16 • M. Lee

▶II
BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"Very powerful tools and concepts!"
-RANDY WAGNER, BASIN ELECTRIC

Who Should Attend

- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center (SOC) team leads and analysts
- ICS red team and penetration testers
- Active defenders

ICS515: ICS Active Defense and Incident Response will help you deconstruct 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 industrial control system 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 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.

You Will Be Able To

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

Author Statement

This class was developed from my experiences in the U.S. intelligence community and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is do-able.

- Robert M. Lee

Auditing & Monitoring Networks, Perimeters, and Systems

SANS AUD507

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Tysons Corner
Oct 24-29 • Risenhoover

CDI
Dec 12-17 • Risenhoover

www.giac.org/gsna

www.sans.edu

WITH THIS COURSE
www.sans.org/ondemand

www.sans.org/8140

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? 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.

"AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!" -Carlos E., U.S. Army

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 either produce or provide you directly 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 five 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. Students are invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

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.

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

SEC440

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Course | 12 CPEs | Laptop NOT Needed

TRAINING EVENTS

Tysons Corner
Oct 22-23 • Marchany

CDI
Dec 10-11 • Marchany

This course will help 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). The 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. The controls were selected and defined by the U.S. military, other government agencies (including the NSA, DHS, GAO, and many others), and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. These entities defined the controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented.

"SEC440 provides an excellent prioritized approach to IT security." -Darrell Bateman, Texas Tech

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

You will find the full document describing the Critical Security Controls posted at the Center for Internet Security at **www.cisecurity.org/critical-controls.cfm**.

Notice: Please note SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.

SEC567

Social Engineering for Penetration Testers

NEW!

Two-Day Course | 12 CPEs | Laptop Required | **TRAINING EVENT: CDI** (Dec 10-11 – Shackleford)

SEC567: Social Engineering for Penetration Testers provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical methods to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks and bolsters this with many examples of what works taken from the experiences of both cyber criminals and the authors. On top of these principles, the course offers a number of tools (produced during the authors' engagements over the years and now available in the course) and labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

You'll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You'll also learn how to conduct pretexting exercises, and we wrap up the course with a fun "Capture the Human" exercise to put what you've learned into practice. This is the perfect course to open up new attack possibilities, better understand the human vulnerability in attacks, and let you practice snares that have proven themselves in tests time and time again.

SECURITY SKILL-BASED COURSE

SEC580
Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | 12 CPEs | Laptop Required | **TRAINING EVENT: CDI** (Dec 10-11 – Galbraith)

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.

MANAGEMENT SKILL-BASED COURSE

MGT305
Technical Communication and Presentation Skills for Security Professionals

One-Day Course | 6 CPEs | Laptop Required | **TRAINING EVENT: CDI** (Dec 11 – Simon)

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, and how to create outstanding presentation materials. Attendees will also get a crash course on advanced public speaking skills.

Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material, we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. We also discuss some of the most common mistakes that can negatively impact the reception of your work and show how to avoid them. Attendees can expect to see the overall quality of their reports improve significantly as a result of this exercise.

After writing a meaningful report, it is not uncommon to find that we must present the key findings from that report before an audience, whether that audience is our department, upper management, or perhaps even the entire organization. How do you transform an excellent report into a powerful presentation? We will work through a process that serves to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.

SANS Technology Institute
www.sans.edu

MGT415

A Practical Introduction to Cyber Security Risk Management

Two-Day Course | 12 CPEs | Laptop Required | **TRAINING EVENT: CDI** (Dec 10-11 – Tarala)

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, 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 assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

MGT433

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Two-Day Course | 12 CPEs | Laptop NOT Needed

TRAINING EVENTS

Tysons Corner
Oct 22-23 • Spitzner

CDI
Dec 10-11 • Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain, and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers as well. Please bring example materials from your security awareness program that you can show and share with other students during the course. 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.

SANS Technology Institute
www.sans.edu

MGT535

Incident Response Team Management

Two-Day Course | 12 CPEs | Laptop Required | **TRAINING EVENT: CDI** (Dec 10-11 – Crowley)

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense.

Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

The course has been updated to address current issues such as the advanced persistent threat, incident response in the cloud, and threat intelligence.

CORE NETWARS TOURNAMENT

In-Depth, Hands-On InfoSec Skills – Embrace the Challenge

The CORE NetWars Tournament is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military agencies are using NetWars to help identify skilled personnel and provide extensive hands-on training. With CORE NetWars, you'll build a wide variety of skills while having a great time.

TRAINING EVENTS

Virginia Beach
Aug 25-26 • Aug 31 - Sep 1 • McJunkin

Pen Test HackFest
Nov 5 & 8 • Staff

CDI
Dec 15-16 • McJunkin

Free when purchasing a four-, five-, or six-day course if NetWars is offered at the same training venue.

DFIR NETWARS TOURNAMENT

Challenge Yourself Before the Enemy Does

The DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It was developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

TRAINING EVENT

CDI
Dec 15-16 • Hagen & J. Williams

Free when purchasing a four-, five-, or six-day course if NetWars is offered at the same training venue.

NETWARS CYBERCITY

TRAINING EVENT

Pen Test HackFest
Nov 7 • Staff

The main objectives of CyberCity are:

- Teach cyber warriors and their leaders the potential kinetic impact of cyber attacks
- Provide a hands-on, realistic kinetic cyber range with engaging missions to conduct defensive and offensive actions
- Develop capabilities for defending and controlling critical infrastructure components to mitigate or respond to cyber attacks
- Demonstrate to senior leaders and planners the potential impact of cyber attacks and cyber warfare

Free when purchasing a four-, five-, or six-day course if NetWars is offered at the same training venue.

5TH ANNUAL

NETWARS TOURNAMENT of CHAMPIONS

HELD DURING CYBER DEFENSE INITIATIVE 2016

WASHINGTON, DC | DEC 15 & 16

Players who earn a top spot in each NetWars Tournament throughout 2016 receive an invitation to the prestigious SANS NetWars Tournament of Champions event.

BONUS SESSIONS

Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

Virginia Beach

KEYNOTE:
Quality Not Quantity: Continuous Monitoring's Deadliest Events – Eric Conrad

Hactivism: Online Protest, Real-World Consequences – Cindy Murphy

Jailbreak / Root Workshop for Mobile Devices – Chris Crowley

HTTPDeux – Adrien de Beaupre

How to Commit Card Fraud – G. Mark Hardy

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls – Kevin Fiscus

KEYNOTE:
The Current Reality: Defending a Compromised Network – Dr. Eric Cole

ICS/SCADA Cyber Attacks - Fact vs. Fiction – Robert M. Lee

Welcome Threat Hunters, Phishermen, and Other Liars – Rob Lee

The Tap House – Philip Hagen

www.sans.org/event/virginia-beach-2016/bonus-sessions

Crystal City

KEYNOTE:
Exploitation 101: Stacks, NX/DEP, ASLR, and ROP! – David Hoelzer

HTTPDeux – Adrien de Beaupre

The Red Pill. Become Aware: Squashing Security Misconceptions and More – My-Ngoc Nguyen

www.sans.org/event/crystal-city-2016/bonus-sessions

Baltimore

KEYNOTE:
Evolving Threats – Paul A. Henry

Continuous Ownage: Why You Need Continuous Monitoring – Bryan Simon

Running Away from Security: Web App Vulnerabilities and OSINT Collide – Micah Hoffman

(Am)Cache Rules Everything Around Me – Eric Zimmerman

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls – Kevin Fiscus

www.sans.org/event/baltimore-2016/bonus-sessions

Pen Test HackFest SUMMIT & TRAINING

Internet of Things

SUMMIT DESCRIPTION

www.sans.org/event/pen-test-hackfest-2016/bonus-sessions

BONUS SESSIONS

Tysons Corner

KEYNOTE:
Evolving Threats
– Paul A. Henry

How to Commit Card Fraud – G. Mark Hardy

The "Know Normal, Find Evil" Series: Windows 10 Memory Forensics Overview – Alissa Torres

www.sans.org/event/tysons-corner-2016/bonus-sessions

Cyber Defense Initiative

KEYNOTE:
What's New for Security in Microsoft Windows Server 2016 and Windows 10?
– Jason Fossen

Securing Your Kids – Lance Spitzner

Security Awareness: Understanding and Managing Your Top Seven Human Risks – Lance Spitzner

GIAC Program Presentation

Quality Not Quantity: Continuous Monitoring's Deadliest Events – Eric Conrad

The iOS of Sauron: How iOS Tracks Everything You Do – Sarah Edwards

Analysis of the Cyber Attack on the Ukrainian Power Grid – Robert M. Lee

Perception Management in Information Warfare – Stephen Northcutt

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls – Kevin Fiscus

How to Build a Cybersecurity Platform the Easy Way – Keith Palmgren

Current and Future Trends in Digital Investigative Analysis – Ovie Carroll

The Tap House – Philip Hagen

Open-Source Intelligence (OSINT) Tips for Malware Investigations – Lenny Zeltser

CISSP - How to Get the Certification that Matters the Most – David R. Miller

www.sans.org/event/cyber-defense-initiative-2016/bonus-sessions

Pen Test HackFest Summit

Crystal City | November 2-3

The Pen Test HackFest is an ideal way to learn offensive techniques so you can better defend your environment. Whether you are a penetration tester, a forensics specialist, or defender, the techniques covered at the HackFest represent the latest and most powerful attacks every organization needs to thwart. Featuring top-rated, industry-leading experts sharing their best tips and advice, this must-attend event is focused on building your skills and providing super high-value in your work. Other hacker and pen test conferences cover interesting hacks, but only the SANS Pen Test HackFest is focused on imparting skills you can directly apply to your next project.

Enhance Your Training Experience

WITH:

Even More Training Value

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

Extend Your Training Experience with OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS Training Formats

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training www.sans.org/private-training
Live Onsite Training at Your Office Location. Both In-Person and Online Options Available

Mentor www.sans.org/mentor
Live Multi-Week Training with a Mentor

Summit www.sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand www.sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive www.sans.org/vlive
Online Evening Courses with SANS' Top Instructors

Simulcast www.sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles www.sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SANS SECURING THE HUMAN

Security Awareness Training by the Most Trusted Source

Computer-based Training for Your Employees

End User
CIP v5/6
ICS Engineers
Developers
Healthcare

- Let employees train on their own schedule
- Tailor modules to address specific audiences
- Courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes

Visit SANS Securing The Human at
securingthehuman.sans.org

Department of Defense Directive 8140

(DoDD 8140)

www.sans.org/dodd-8140

Department of Defense Directive 8570 has been replaced by the DoD CIO and is now DoDD 8140. DoDD 8570 is now part of a larger initiative that falls under the guidelines of DoDD 8140. DoDD 8140 provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC certifications are among those required for Technical, Management, CND, and IASAE classifications.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III	IAM Level I	IAM Level II	IAM Level III
A+CE Network+CE SSCP	**GSEC** (SEC401) Security+CE SSCP	**GCED** (SEC501) **GCIH** (SEC504) **CISSP** (MGT414) (or Associate) CISA	**GSLC** (MGT512) CAP Security+CE	**GSLC** (MGT512) **CISSP** (MGT414) (or Associate) CAP, CASP CISM	**GSLC** (MGT512) **CISSP** (MGT414) (or Associate) CISM

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA (SEC503) **GCIH** (SEC504) CEH	SSCP CEH	**GCIH** (SEC504) **GCFA** (FOR508) CSIH, CEH	**GSNA** (AUD507) CISA CEH	CISSP - ISSMP CISM

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I	IASAE II	IASAE III
CISSP (MGT414) (or Associate)	**CISSP** (MGT414) (or Associate) CASP	CISSP - ISSEP CISSP - ISSAP

Computer Environment (CE) Certifications

GCWN (SEC505) **GCUX** (SEC506)

Compliance/Recertification:

To stay compliant with DoDD 8140 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to www.giac.org to learn more about certification renewal.

SANS Training Courses for DoDD-Approved Certifications

SANS TRAINING COURSE		DoDD-APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	GCIH
SEC505	Securing Windows and PowerShell Automation	GCWN
SEC506	Securing Linux/Unix	GCUX
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Digital Forensics and Incident Response	GCFA
MGT414	SANS Training Program for CISSP® Certification	CISSP
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	GSLC

DoDD 8140 certification requirements are subject to change, please visit **http://iase.disa.mil/eta/iawip** for the most updated version.

For more information, contact us at **8570@sans.org** or visit **www.sans.org/8140**

HOTEL INFORMATION

COMMUNITY SANS CHANTILLY

Hyatt Place CHANTILLY DULLES AIRPORT – SOUTH
4994 Westone Plaza | Chantilly, VA 20151
703-961-8160

Special Hotel Rates Available: $119.00*

For hotel information, visit www.sans.org/community

COMMUNITY SANS RICHMOND

Courtyard RICHMOND WEST
6400 West Broad Street | Richmond, VA
804-282-1881

Special Hotel Rates Available: $149.00*

For hotel information, visit www.sans.org/community

VIRGINIA BEACH

Hilton VIRGINIA BEACH OCEANFRONT
3001 Atlantic Avenue | Virginia Beach, VA 23451 | 757-213-3000

Special Hotel Rates Available: $199.00*

Good through July 22nd

For hotel information, visit www.sans.org/event/virginia-beach-2016/location

CRYSTAL CITY

DoubleTree by Hilton WASHINGTON DC-CRYSTAL CITY
300 Army Navy Drive | Arlington, VA 22202 | 703-416-4100

Special Hotel Rates Available: $169.00*

Good through August 14th

For hotel information, visit www.sans.org/event/crystal-city-2016/location

SANS MENTOR – ARLINGTON

Residence Inn ARLINGTON ROSSLYN
1651 North Oak Street | Iwo Jima Room | Arlington, VA 22209

For hotel information, visit www.marriott.com/hotels/travel/wasrr-residence-inn-arlington-rosslyn

BALTIMORE

Sheraton INNER HARBOR
300 South Charles Street | Baltimore, MD 21201 | 410-962-8300

Special Hotel Rates Available: $205.00*

Good through September 9th

For hotel information, visit www.sans.org/event/baltimore-2016/location

TYSONS CORNER

Hilton McCLEAN TYSONS CORNER
7920 Jones Branch Drive | McClean, VA 22102 | 703-847-5000

Special Hotel Rates Available: $204.00*

Good through September 30th

For hotel information, visit www.sans.org/event/tysons-corner-2016/location

PEN TEST HACKFEST

DoubleTree by Hilton WASHINGTON DC-CRYSTAL CITY
300 Army Navy Drive | Arlington, VA 22202 | 703-416-4100

Special Hotel Rates Available: $179.00*

Good through October 9th

For hotel information, visit www.sans.org/event/pen-test-hackfest-2016/location

CYBER DEFENSE INITIATIVE

Grand Hyatt WASHINGTON
1000 H Street NW | Washington, DC 20001
202-582-1234

Special Hotel Rates Available: $219.00*
Good through November 18th

WASHINGTON **Marriott** AT METRO CENTER
775 12th Street NW | Washington DC 20005
202-737-2200

Special Hotel Rates Available: $179.00*
Good through November 13th

For hotel information, visit www.sans.org/event/cdi-2016/location

*Price will be honored based on space availability

REGISTRATION INFORMATION

REGISTER ONLINE

Select your course or courses and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

We recommend you register early to ensure you get your first choice of courses.

Pay Early and Save

Some restrictions apply.

Use code **EarlyBird16** when registering early

Event	Save $400 by paying before	Save $200 by paying before	No refunds after
COMMUNITY SANS **Columbia** (SEC401)	Jun 8	Jun 30	Jul 13
COMMUNITY SANS **Chantilly** (SEC504)	Jun 15	Jul 6	Jul 20
COMMUNITY SANS **Columbia** (SEC560)	Jun 22	Jul 13	Jul 27
COMMUNITY SANS **Columbia** (SEC504)	Jun 29	Jul 20	Aug 3
Virginia Beach	Jun 29	Jul 20	Aug 3
COMMUNITY SANS **Columbia** (FOR572)	Jul 6	Jul 27	Aug 10
Crystal City	Jul 13	Aug 3	Aug 17
COMMUNITY SANS **Columbia** (SEC401)	Aug 3	Aug 17	Aug 31
COMMUNITY SANS **Columbia** (SEC501)	Aug 10	Aug 24	Sep 7
SANS MENTOR – **Arlington**	Aug 16	Aug 30	Sep 13
Baltimore	Aug 17	Sep 7	Sep 21
COMMUNITY SANS **Columbia** (FOR508)	Aug 17	Sep 7	Sep 21
COMMUNITY SANS **Chantilly** (SEC401)	Aug 17	Sep 7	Sep 21
Tysons Corner	Aug 31	Sep 21	Oct 5
COMMUNITY SANS **Richmond** (SEC401)	Sep 7	Sep 21	Oct 5
COMMUNITY SANS **Chantilly** (SEC301)	Sep 14	Sep 28	Oct 12
Pen Test HackFest SUMMIT & TRAINING	Sep 20	Oct 4	Oct 18
Cyber Defense Initiative (CDI)	Oct 19	Nov 9	Nov 23
COMMUNITY SANS **Richmond** (SEC504)	Oct 26	Nov 16	Nov 30

SANS VOUCHER PROGRAM

The SANS Voucher Program allows an organization to manage its training budget from a single SANS Account, potentially receive bonus funds based on its investment level, and centrally administer its training. www.sans.org/vouchers

Open a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert 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 to show how a vendor's commercial tool can be used to solve or mitigate that problem.

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

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- 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)

sans.org/security-resources