THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Security East 2016

New Orleans, LA | January 25-30

Choose from these popular courses:

NEW! Web App Penetration Testing and Ethical Hacking

NEW! ICS Active Defense and Incident Response

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Windows Forensic Analysis

Intrusion Detection In-Depth

And more!

"SANS has excellent applicable material that is well presented, and the training gives me real-world skills I can apply immediately!"

-Mark Burns, LG&E-KU

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

Register at
sans.org/security-east-2016

SAVE $400
by registering & paying early!
See page 21 for more details.

SANS Security East 2016 is back in the "Big Easy" on January 25-30. Here's your chance to improve your skills in IT security, forensics, pen testing, incident handling, and security management. Staying ahead of persistent security threats requires diligence and practical, innovative training. SANS' top-rated courses will provide you with the skills you'll need to meet the challenges ahead.

The SANS Security East 2016 brochure highlights each of the courses offered as well as our line-up of instructors, including Eric Conrad, Seth Misenar, Mike Poor, James Tarala, Christopher Crowley, Kevin Fiscus, G. Mark Hardy, Robert M. Lee, Michael Murr, Bryan Simon, Alissa Torres, and David Cowen. SANS instructors are experienced industry practitioners with the expertise to provide you with top-rated security training that you can apply the day you get back to the office.

SANS Technology Institute is regionally accredited and eligible for tuition reimbursement plans, and offers master's degrees as well as graduate certificates in specialized fields such as penetration testing or incident response. To learn more, see page 15.

Cyber professionals who hold **GIAC** certifications are recognized as experts in the IT industry and are sought after by government, military, and industry. To learn how to put your skills to practical use, join the GIAC certified professionals that protect the cyber environment. See page 14 for more information.

When completing the online registration form, be sure to add an **OnDemand Bundle** to your course at a reduced rate. SANS OnDemand Bundles get you four months of online access to your course's custom e-learning program, lecture video or audio files, quizzes, and labs – all accessible through your SANS portal account after your live training ends (ICS515 is not available).

Our SANS Security East 2016 campus is at the **Hilton New Orleans Riverside**, in the heart of the Big Easy. The riverfront hotel is on the banks of the Mississippi, steps away from the famous New Orleans Streetcar lines, and a few blocks from the French Quarter. You can stroll through a plantation, shop at Riverwalk Marketplace, take a swamp tour, choose from over 45 museums, and experience unique dining at some of the city's best restaurants. New Orleans is an extraordinary destination with something of interest for everyone! A special discounted rate of $199 S/D will be honored based on space availability through January 1, 2016.

Register and pay for any Security East course by December 2, 2015 and save $400 by entering the discount code **EarlyBird16**.

Join us in New Orleans for SANS Security East 2016 for the best security training your money can buy – we are looking forward to meeting you in New Orleans!

SANS

Here is what last year's attendees had to say:

"Great material. It validated that I've had the right idea with these topics over the last several years! I now have a few new tools to add to my set that I had previously overlooked."
-Torry Crass,
SPX Corporation

"This course has helped strengthen my skills in forensics and incident response through understanding concepts in IR. I have also learned how to use the full potential of various tools."
-Louise Cheung,
Stroz Friedberg

"I felt like, when I entered this classroom, I was a recruit still wet behind the ears. But when I left, I was a special-forces sniper!"
-Jack Baylor, Qualcomm

Courses-at-a-Glance

		MON 1-25	TUE 1-26	WED 1-27	THU 1-28	FRI 1-29	SAT 1-30
SEC401	**Security Essentials Bootcamp Style**	Page 1	■	■	■	■	■
SEC503	**Intrusion Detection In-Depth**	Page 2	■	■	■	■	■
SEC504	**Hacker Tools, Techniques, Exploits, and Incident Handling**	Page 3	■	■	■	■	■
SEC511	**Continuous Monitoring and Security Operations**	Page 4	■	■	■	■	■
SEC542	**Web App Penetration Testing and Ethical Hacking NEW!**	Page 5	■	■	■	■	■
SEC560	**Network Penetration Testing and Ethical Hacking**	Page 6	■	■	■	■	■
SEC566	**Implementing and Auditing the Critical Security Controls**	Page 7	■	■	■	■	
SEC575	**Mobile Device Security and Ethical Hacking**	Page 8	■	■	■	■	■
FOR408	**Windows Forensic Analysis**	Page 9	■	■	■	■	■
FOR526	**Memory Forensics In-Depth**	Page 10	■	■	■	■	■
MGT512	**SANS Security Leadership Essentials For Managers with Knowledge Compression™**	Page 11	■	■	■	■	
ICS515	**ICS Active Defense and Incident Response NEW!**	Page 12	■	■	■	■	

@SANSInstitute *Join the conversation:* **#SecurityEast**

SEC401:

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"SEC401 is what I was looking forward to and I was not disappointed! I can say without a doubt that I have action items each day in class that I can take back to work and in my personal life."
-Ed Burkett, CUSO Financial

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.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This 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 advanced persistent threat, 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'll 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.

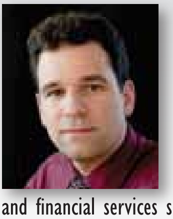
GIAC SECURITY ESSENTIALS GSEC
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

▶❚❚ Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand



Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 11 GIAC certifications, including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and acceptance into the prestigious SANS Cyber Guardian program. @BryanOnSecurity

SANS

SEC503:

Intrusion Detection In-Depth

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Poor

- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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?

Who Should Attend

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

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.

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.

"The material was presented in a way that facilitates understanding rather than just memorization."
-Edward Dunnahoe, CRIF Lending Solutions

"Excellent exposure and training for all skill levels. Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

GIAC CERTIFIED INTRUSION ANALYST GCIA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

▶II Bundle OnDemand with this course
sans.org/ondemand

Mike Poor *SANS Senior Instructor*

Mike Poor is a founder and senior security analyst for the Washington, DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is on intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling "Snort" series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center. @Mike_Poor

SANS

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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.

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, 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 for, 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.

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- 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

"The instructor opened my eyes and helped me understand how to approach the concepts of offensive security and incident handling."
-Stephen Ellis, CB&I

"The instructor's passion for this topic has influenced me to pursue this area further and to increase my skills. This has been a great experience and the labs were immensely important."
-Stephen M., Army National Guard

GIAC CERTIFIED INCIDENT HANDLER GCIH
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

▶ II
Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SEC504: Hacker Tools, Techniques, Exploits and Incident Handling; FOR508: Advanced Digital Forensics and Incident Response; and FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques. He has also led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-east-2016

SEC511:

Continuous Monitoring and Security Operations

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

- GIAC Cert: GMON
- Master's Program
- OnDemand Bundle

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

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 is 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.

Who Should Attend

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

giac.org

sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"It is only day one and I already know SEC511 will arm me with the knowledge I need to lead my security program to effectively defend my organization."
-Stacey Boivin, Alberta Electric System Operator

"SEC511 is a practical approach to continue security monitoring using free and open-source tools either alone or in conjunction with existing tools and devices. This course is a must for anyone responsible for monitoring networks for security."
-Brad Milhorn, CompuCom

Eric Conrad *SANS Senior Instructor*

Eric Conrad is the lead author of SANS MGT414: SANS Training Program for CISSP® Certification, and coauthor of both SANS SEC511: Continuous Monitoring and Security Operations and SANS SEC542: Web App Penetration Testing and Ethical Hacking. He is also the lead author of the *CISSP Study Guide*, and the *Eleventh Hour CISSP: Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now CTO of Backshore Communications, a company focusing on hunt teaming, intrusion detection, incident handling, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com. @eric_conrad

SEC542:

Web App Penetration Testing and Ethical Hacking

NEW

SANS

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar

- GIAC Cert: GWAPT
- STI Master's Program
- OnDemand Bundle

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.

Who Should Attend

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

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, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

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

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the 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.

GIAC Web Application Penetration Tester GWAPT
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

▶❚❚ BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

> "As with all SANS training I've taken, even when I think I know the subject well I'm learning something new."
> -Benjamin Bagby, XE.com

> "The instructor's knowledge gave me a better perspective on the development process, and helped peel back the onion on infrastructure and environments. This has taught me how to think outside of the box."
> -Ephraim P., USAF

Seth Misenar *SANS Senior Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security thought leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include the CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-east-2016

SEC560:

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program

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 duty head-on.

SEC560 is the must-have course for every well-rounded security professional.

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

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

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

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

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

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

"This course has a direct correlation to my job duties. The insight, real-world references, and the use of various tools will make my job a lot easier. You will learn skills and ways your systems are vulnerable."
-Roland Thomas, USAF

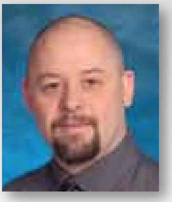
"SEC560 really tests your skills and abilities and the Netcat backdoor exercises have really opened my eyes on the endless possibilities & capabilities."
-David Poulin, 7th Cyber Protection Brigade

GIAC PENETRATION TESTER GPEN
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

▶II
Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand



Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414. @kevinbfiscus

SANS

SEC566:

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
Mon, Jan 25 - Fri, Jan 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala

- GIAC Cert: GCCC
- Masters Program

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

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

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?

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.

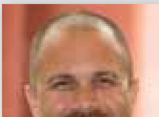
The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical 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.

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. Specifically, by the end of the course students will know how to:

- Create a strategy to successfully defend their data
- Implement controls to prevent data from being compromised
- Audit systems to ensure compliance with Critical Control standards.

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.



James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a featured speaker for the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them with their security management, operational practices, and regulatory compliance, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. @isaudit

SEC575:

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Christopher Crowley

- GIAC Cert: GMOB
- STI Master's Program
- OnDemand Bundle

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning (ERP) to project management.

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- The high probability of device loss or theft, and more

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

SEC575: Mobile Device Security and Ethical Hacking is designed to help organizations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course will help you build the critical skills to support your organization's secure deployment and use of mobile phones and tablets. You will learn how to capture and evaluate mobile device network activity, disassemble and analyze mobile code, recognize weaknesses in common mobile applications, and conduct full-scale mobile penetration tests.

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

GIAC MOBILE DEVICE SECURITY ANALYST GMOB
giac.org

SANS Technology Institute
sans.edu

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

"Chris is an awesome instructor! Quick to answer questions, very knowledgeable and gave great examples and stories."
-Katrina Howard, Booz Allen & Hamilton

"Once again, SANS has exceeded my expectations and successfully re-focused my view of threats and risks. I recommend this course because it is very enlightening."
-Charles Allen, EM Solutions, Inc.

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Chris is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor-of-the-Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

SANS

FOR408:
Windows Forensic Analysis

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Cowen

- GIAC Cert: GCFE
- STI Master's Program
- OnDemand Bundle

DFIR
digital-forensics.sans.org

"After the course, I am able to have a good picture of the whole process from the basic hands-on to the organizations of findings. Excellent!"
-Jenny Blaine, University of Minnesota

"FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations."
-Nathan Lewis, KPMG

Master Windows Forensics – You can't protect what you don't know about.

Who Should Attend

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

Every organization 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.

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 know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. 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. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving 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, Windows 8/8.1, 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 8.1 artifacts.

GIAC Certified Forensic Examiner GCFE
giac.org

SANS Technology Institute
sans.edu

▶❚❚ Bundle OnDemand
with this course
sans.org/ondemand

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME

David Cowen *SANS Instructor*

David Cowen is a Partner at G-C Partners, LLC, where his team of expert digital forensics investigators pushes the boundaries of what is possible on a daily basis. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sector. His work has involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series of books on digital forensics: *Hacking Exposed Computer Forensics* (1st-3rd Editions), *Infosec Pro Guide to Computer Forensics*, and the *Anti Hacker Toolkit* (3rd Edition). His research into file system journaling forensics has created a new area of analysis that is changing the industry. Combined with Triforce products, David's research enables examiners to go back in time to find previously unknown artifacts and system interactions. David speaks about digital forensics and file system journaling forensics at DFIR and Infosec conferences across the United States. He has taught digital forensics both as a SANS instructor and as a graduate instructor at Southern Methodist University. @hecfblog

FOR526:

Memory Forensics In-Depth

Six-Day Program
Mon, Jan 25 - Sat, Jan 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Alissa Torres
▸ OnDemand Bundle

DFIR
digital-forensics.sans.org

"After spending a few days in class, I'm very excited to learn that there is so much data available, and I like the fact that there are lots of hands-on things to do. An ounce of practical experience is worth more than a pound of theory. I'm going to go and try this at work!"
-Greg Dub, National Center for Policy Analysis

"This course is totally awesome, relevant, and eye opening. I want to learn more every day."
-Matthew Britton, Blue Cross Blue Shield of Louisiana

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

Who Should Attend

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

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

MALWARE CAN HIDE, BUT IT MUST RUN

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

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

You Will Learn:

- Proper Memory Acquisition
- How to Find Evil in Memory
- Effective Step-by-Step Memory Analysis Techniques
- Best Practice Techniques

▶II
Bundle OnDemand
with this course
sans.org/ondemand

Alissa Torres *SANS Certified Instructor*

Alissa Torres specializes in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+. @sibertor

SANS

MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, Jan 25 - Fri, Jan 29
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: G. Mark Hardy

- GIAC Cert: GSLC
- STI Master's Program
- DoDD 8570
- OnDemand Bundle

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.

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.

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

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!

"This was a great course! I feel all management should take it because it helps managers understand not only security but also technical and business concepts and issues."
-David Stewart, ADM

"Mark is a wealth of knowledge and experience which adds value to the class. His injection of real-world scenarios as he is teaching is very helpful."
-Pam L., National Nuclear Security Administration

GIAC Security Leadership Certification GSLC
giac.org

SANS Technology Institute
sans.edu

sans.org/8570

▶❚❚ Bundle OnDemand
with this course
sans.org/ondemand

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM, and CISA certifications. @g_mark

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-east-2016

ICS515:

ICS Active Defense and Incident Response

NEW

Five-Day Program
Mon, Jan 25 - Fri, Jan 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

ICS515: ICS Active Defense and Incident Response will empower students to understand their networked industrial control system (ICS) environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats is known as "active defense." It is the approach needed to appropriately 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 fully understanding how to to deconstruct targeted ICS attacks, with a focus on delivery methods and observable attributes. This knowledge demystifies adversary capabilities and gives actionable recommendations to defenders. The course uses a hands-on approach that shows real-world malware and breaks down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of concepts such as generating and using threat intelligence, performing network security monitoring, and executing threat triage and incident response to ensure the safety and reliability of operations. The strategy presented in the course serves as a basis for ICS organizations looking to show that defense is doable.

Who Should Attend

- Information Technology and Operational Technology (IT and OT) cybersecurity personnel
- IT and OT support personnel
- ICS incident responders
- ICS engineers
- Security Operations Center personnel

"Awesome course!! Rob's explanation around the labs was comprehensive and the concepts were explained really well. Where was Rob hiding until this course?"
-Srinath Kannan, Accenture

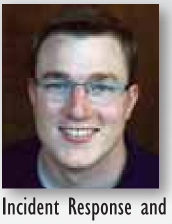
"ICS environments are unique and require specialized skills and processes to effectively manage the threats and vulnerabilities."
-John Ballentine, EthosEnergy

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 doable."
-Robert M. Lee

What You Will Receive

A fully functioning ICS515 CYBATIWorks Mini-Kit that students take with them after the class. The kit includes a Raspberry PI that functions as a PLC, physical components and attachments for I/O, a virtual machine with commercial control system demonstration software from Rex Controls and PeakHMI, and industrial protocols and software including OPC, ModbusTCP, DNP3, and more.



Robert M. Lee *SANS Certified Instructor*

Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. He is a passionate educator although he should not be confused with the other Rob Lee at SANS – that Rob Lee is cooler but has less hair. Robert obtained his start in cybersecurity in the U.S. Intelligence Community, where he served as an Air Force Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations and established a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles and journals in publications such as Control Engineering, Wired, and Passcode and is a frequent speaker at conferences around the world. He is a non-resident National Cyber Security Fellow at the New America think tank and is currently pursuing his PhD at Kings College London with research into the cybersecurity of control systems. Robert is the author of the book *SCADA and Me* and the weekly web-comic www.LittleBobbyComic.com @RobertMLee

BONUS SESSIONS – EVENING TALKS

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.

KEYNOTE: Data Theft in the 21st Century *Mike Poor*

A state-of-the-industry look into theft and exposure of huge data sets of PII and PEI (personally embarrassing and exposing information).

Continuous Ownage: Why you Need Continuous Monitoring

Eric Conrad and Seth Misenar

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Eric Conrad and Seth Misenar's course: SANS SEC511: Continuous Monitoring and Security Operations.

Card Fraud 101 *G. Mark Hardy*

Ever get a call from your bank saying your credit card was stolen, but it was still in your wallet? What's going on here? Card fraud costs $16 billion annually, and it's not getting better. Target, PF Changs, Michaels, Home Depot, who's next? Find out how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and how crooks compromised Apple Pay. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

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

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data are destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information, however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

Using an Open-Source Threat Model for Prioritized Defense

James Tarala

Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors – so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization's defenses – without all the confusion. In this presentation James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk it faces. Then he will show how to practically use this model to prioritize enterprise defense and map to existing compliance requirements facing organizations today. Whether you are in the Department of Defense or work for a small mom-and-pop retailer, you will be able to use this model to specifically determine a prioritized defense for your organization.

Understanding Your ICS Topologies *Robert M. Lee*

In this presentation Robert M. Lee will discuss how to understand your ICS topologies to include data flows, asset identification, and the visualization of your network. This critical component of security plays a significant role in defense of the network as well as in terms of the fundamental situational awareness required for the configuration and safe operation of networked devices. The talk will include recommended methodologies and available tools to help address this issue while showcasing why the need is so vital.

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

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

SPECIAL PRICING

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.

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

OnDemand Bundles and GIAC certifications are not available for all courses

Department of Defense Directive 8570

(DoDD 8570)

sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) 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 provides the most options in the industry for meeting 8570 requirements.

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 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to 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 with PowerShell and the Critical Security Controls	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 8570 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 sans.org/8570

SANS CYBER GUARDIAN PROGRAM

sans.org/cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification. Contact us at **privatetraining@sans.org** to get started!

Program Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above)
  or
  CISSP certification

Core Courses

SEC503	Intrusion Detection In-Depth (GCIA)
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling (GCIH)
SEC560	Network Penetration Testing and Ethical Hacking (GPEN)
FOR508	Advanced Digital Forensics and Incident Response (GCFA)

After completing the core courses, students must choose one course and certification from either the Blue or Red Team

Blue Team Courses

SEC502	Perimeter Protection In-Depth (GPPA)
SEC505	Securing Windows with PowerShell and the Critical Security Controls (GCWN)
SEC506	Securing Linux/Unix (GCUX)

Red Team Courses

SEC542	Web App Penetration Testing and Ethical Hacking (GWAPT)
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (GXPN)

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

Top 5 Reasons

why SANS customers use CyberTalent Assessments to manage their cyber talent.

1

SANS Leadership

SANS is the most trusted and the largest source for information security training and certification in the world.

2

Reduce Hiring Costs

CyberTalent Assessments provide more information and better insight, which reduces your risk of costly hiring mistakes.

3

Better Team Management

A simple, easy-to-use tool that helps you identify your team's specific needs, map your talent portfolio, and develop personalized training plans for each member of your team.

4

Ensure Contractor Skills

CyberTalent Assessments provide a reliable, effective way to be sure your contractor have the skills you need.

5

Prepare for Today's Threats

CyberTalent Assessments help ensure your team is ready for the changing threat landscape.

SANS CyberTalent offers three web-based assessments:

- Cyber Defense
- Penetration Testing
- Digital Forensics

Start improving your cyber talent management today. There's no reason to wait.

SANS | CyberTalent

sans.org/cybertalent

Contact: dbrown@sans.org or mshuftan@sans.org

Sign up for a FREE demo

sans.org/cybertalent/free-demo

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

sans.org/community

Private Training

Your Location! Your Schedule!

sans.org/private-training

Mentor

Live Multi-Week Training with a Mentor

sans.org/mentor

Summit

Live IT Security Summits and Training

sans.org/summit

ONLINE TRAINING

OnDemand

E-learning Available Anytime, Anywhere, at Your Own Pace

sans.org/ondemand

vLive

Online, Evening Courses with SANS' Top Instructors

sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

sans.org/simulcast

OnDemand Bundles

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

FUTURE SANS TRAINING EVENTS

SANS South Florida 2015
Fort Lauderdale, FL | November 9-14

SANS Pen Test Hackfest SUMMIT & TRAINING
Alexandria, VA | November 16-23

SANS San Francisco 2015
San Francisco, CA | November 30 - December 5

SANS Security Leadership SUMMIT & TRAINING
Dallas, TX | December 3-10

SANS Cyber Defense Initiative 2015
Washington, DC | December 12-19

SANS Las Vegas 2016
Las Vegas, NV | January 9-14

SANS Scottsdale 2016
Scottsdale, AZ | February 8-13

SANS McLean 2016
McLean, VA | February 15-20

ICS Security SUMMIT & TRAINING
Orlando, FL | February 16-23

SANS Anaheim 2016
Anaheim, CA | February 22-27

SANS Philadelphia 2016
Philadelphia, PA | February 29 - March 5

SANS 2016
Orlando, FL | March 12-21

SANS Reston 2016
Reston, VA | April 4-9

SANS Atlanta 2016
Atlanta, GA | April 4-9

Threat Hunting and Incident Response SUMMIT & TRAINING
New Orleans, LA | April 12-19

SANS Pen Test Austin 2016
Austin, TX | April 18-23

SANS Security West 2016
San Diego, CA | May 1-6

The latest information on all events can be found at sans.org/security-training/by-location/all

SANS SECURITY EAST 2016

Hotel Information

Training Campus
Hilton New Orleans Riverside

Two Poydras Street
New Orleans, LA 70130
504-561-0500
sans.org/event/security-east-2016/location

Stay in the center of it all at Hilton New Orleans Riverside and enjoy a prime downtown location at the base of Canal and Poydras Streets. Our riverfront hotel is ideally situated next to Harrah's Casino, steps from famous New Orleans Streetcar lines, and a short four-block walk away from the French Quarter, as well as many other iconic landmarks. This downtown New Orleans hotel is also adjacent to the Cruise Terminal, for cruise enthusiasts.

Special Hotel Rates Available

A special discounted rate of $199.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through Jan. 1, 2016.

Top 5 reasons to stay at the Hilton New Orleans Riverside

1 All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.

2 No need to factor in daily cab fees and the time associated with travel to alternate hotels.

3 By staying at the Hilton New Orleans Riverside, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.

4 SANS schedules morning and evening events at the Hilton New Orleans Riverside that you won't want to miss!

5 Everything is in one convenient location!

SANS SECURITY EAST 2016

Registration Information

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

Register online at sans.org/event/security-east-2016/courses

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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**12-2-15**	**$400.00**	**12-23-15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time

5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by January 6, 2016 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers