

SANS Security West 2014

San Diego, CA | May 8-17

EMERGING TRENDS IN CYBERSECURITY

Choose from these popular courses:

Security Essentials Bootcamp Style
Hacker Techniques, Exploits, and Incident Handling
Network Penetration Testing and Ethical Hacking
Computer Forensic Investigations – Windows In-Depth
Security Leadership Essentials For Managers

Plus these NEW courses:

Intrusion Detection In-Depth
Advanced Exploit Development for Penetration Testers
Advanced Network Forensics and Analysis
Advanced Smartphone Forensics

And much more!

*"This training increases my
marketability in the job market.
It also adds value to
my organization."*

-PHILLIP BACA, DRIVE SAVERS DATA RECOVERY



GIAC Approved Training

Register at

www.sans.org/event/sans-security-west-2014

**Save
\$400**

by registering early!

See page 37 for more details.

SANS will return to San Diego for **SANS Security West 2014**

– **Emerging Trends** running from **May 8-17**. This training event will offer almost 30 outstanding hands-on immersion courses for all security professionals in audit, security management, technical security, penetration testing, and computer forensics. The training team will be led by SANS world-class Faculty Fellows Jason Fossen, David Hoelzer, Rob Lee, and Ed Skoudis, as well as Senior Instructors Paul A. Henry, Mike Poor, Stephen Sims, and James Tarala.



This brochure is designed to provide you with all of the information you need to choose the courses at SANS Security West 2014 that best fit your training needs. The course descriptions are descriptive and thorough, so please share the brochure with your colleagues or your boss to help them understand all that you will learn when you attend.

SANS Security West 2014 features evening talks and a star-studded panel discussions regarding emerging trends – *Will The Real Next-Generation Security Please Stand Up?* moderated by John Pescatore. The top trends will also be discussed at two other panel presentations – *Emerging Trends: Offense Informs Defense* and *Emerging Trends in DFIR*. Tweet your thoughts and predictions for **Emerging Trends in 2014** to **#SecWestTrends** or visit **SANS.org/SecWest-Trends**.

Look for our complete list of evening talks, special events, vendor expo, welcome reception, and all of the networking opportunities that provide the ultimate SANS experience to both reinforce and enhance your training. Plus, you don't want to miss participating in **Core NetWars** or **DFIR NetWars** tournaments! The SANS promise is that you will not only learn how to use your problem-solving skills and technical knowledge in a safe environment, you will also be able to apply what you learn the minute you get back to your office.

Please review the complete training list on the **Courses-at-a-Glance** page. Our new cutting-edge courses being offered at SANS Security West 2014 are:

SEC760: Advanced Exploit Development for Penetration Testers

FOR572: Advanced Network Forensics and Analysis

FOR585: Advanced Smartphone Forensics

MGT415: A Practical Introduction to Risk Assessment

Be sure to register and pay by March 12th for a \$400 tuition discount!

Finally, have you been thinking about earning a master's degree? Then the SANS Technology Institute degree programs may be of interest to you. The SANS Technology Institute is a regionally accredited, postgraduate institution focused solely on cybersecurity education for working professionals. Learn more at **www.sans.edu**. The brochure also provides information about earning **GIAC Certification** with your training.

SANS Security West 2014 will be held at the fabulous **Manchester Grand Hyatt Hotel** on the waterfront in San Diego. This destination location offers a retreat for the whole family. Explore Seaport Village, cruise the bay, walk to the Gaslamp Quarter, or visit the San Diego Zoo, Sea World, or the museums in Balboa Park.

Hone your cyber skills while experiencing the best that Southern California has to offer. Make your reservations now! A special discount rate of \$210 Single/Double will be honored based on space availability, but it is only available through April 19, 2014. Government per diem rooms are available with proper ID; simply call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room. Register today for SANS Security West 2014, and we will see you in San Diego!

Here's what SANS alumni have said about the value of SANS training:

"As an incident handler, FOR610 puts me on a more even footing and adds insight into this aspect of incident handling."

-David Quigley, NATO

"Needing to cover so much material quickly, it's important the instructor also keeps it entertaining and informative—




Seth nails it!"

-Mike O'Donnell, Kareo

"The tools and methods in the SEC503 exercises will be immediately useful on the job."

-David Torrey, ThermoAnalytics, Inc.

COURSES-AT-A-GLANCE

			THU 5/8	FRI 5/9	SAT 5/10	SUN 5/11	MON 5/12	TUE 5/13	WED 5/14	THU 5/15	FRI 5/16	SAT 5/17
SEC301: Intro to Information Security					Page 2							
SEC401: Security Essentials Bootcamp Style 					Page 3							
SEC434: Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting		Page 23										
SEC501: Advanced Security Essentials – Enterprise Defender 					Page 4							
SEC503: Intrusion Detection In-Depth NEW!					Page 5							
SEC504: Hacker Techniques, Exploits, and Incident Handling 					Page 6							
SEC505: Securing Windows with the Critical Security Controls					Page 7							
SEC524: Cloud Security Fundamentals		Pg 23										
SEC542: Web App Penetration Testing and Ethical Hacking					Page 8							
SEC546: IPv6 Essentials											Pg 24	
SEC560: Network Penetration Testing and Ethical Hacking					Page 9							
SEC566: Implementing and Auditing the Twenty Critical Security Controls – In-Depth					Page 10							
SEC575: Mobile Device Security and Ethical Hacking					Page 11							
SEC580: Metasploit Kung Fu for Enterprise Pen Testing											Pg 24	
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses					Page 12							
SEC760: Advanced Exploit Development for Penetration Testers NEW!					Page 13							
FOR408: Computer Forensic Investigations – Windows In-Depth					Page 14							
FOR508: Advanced Computer Forensic Analysis and Incident Response					Page 15							
FOR572: Advanced Network Forensics and Analysis NEW! 					Page 16							
FOR585: Advanced Smartphone Forensics NEW!					Page 17							
FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques					Page 18							
MGT305: Technical Communication and Presentation Skills for Security Professionals		Pg 25										
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam					Page 19							
MGT415: A Practical Introduction to Risk Assessment NEW!		Pg 25										
MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program 		Page 25										
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™					Page 20							
AUD444: Auditing Security and Controls of Active Directory and Windows					Page 22							
AUD445: Auditing Security and Controls of Oracle Database								Page 22				
AUD507: Auditing Networks, Perimeters, and Systems					Page 21							



COURSE IS ALSO AVAILABLE ONLINE VIA SIMULCAST – PAGE 36

Intro to Information Security

Five-Day Program
Sat, May 10 - Wed, May 14
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Fred Kerby
► GIAC Cert: GISF

Course updated
to include
hands-on labs!

SANS

"I work in law enforcement which sees cyber attacks as the next big threat to the homeland. SEC301 is providing a good basic foundation of concept to understand how individuals are committing cyber crimes."

-Natalie Villegas, DOJ

"SEC301 provided me with an excellent review and brought to my attention some necessary changes to our network security."

-Terry Benes, University of Nebraska Foundation

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management.

Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss Internet Protocol, routing, Domain Name Service, and network devices. We cover the basics of cryptography, security management, and wireless technology, then we look at policy as a tool to effect change in your organization. On the final day of the course, we put it all together with an implementation of defense in-depth.

If you're a newcomer to the field of information security, this is the course for you! SEC301 will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.



www.giac.org



Fred Kerby SANS Senior Instructor

Fred is an engineer, manager, and security practitioner whose experience spans several generations of networking. He was the Information Assurance Manager at the Naval Surface Warfare Center, Dahlgren Division for more than 16 years and has vast experience with the political side of security incident handling. His team is one of the recipients of the SANS Security Technology Leadership Award as well as the Government Technology Leadership Award. Fred received the Navy Meritorious Civilian Service Award in recognition of his technical and management leadership in computer and network security.

Tweet your predictions for Emerging Trends in 2014 to #SecWestTrends or visit SANS.org/SecWest-Trends

Register at www.sans.org/event/sans-security-west-2014 | 301-654-SANS (7267)

Security Essentials Bootcamp Style

Six-Day Program

Sat, May 10 - Thu, May 15

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

Laptop Required

46 CPE/CMU Credits

Instructor: Keith Palmgren

► GIAC Cert: GSEC

► Masters Program

► Cyber Guardian

► DoDD 8570



SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 36.

"I would strongly recommend SEC401 to IT professionals looking to enhance their skills, knowledge, and abilities on cybersecurity."

-Chris Norwood,
Lockheed Martin

"SEC401 is the best InfoSec training bar none. The value for the money is unbeatable!"

-Ron Fought,
Sirius Computer Solutions



SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems. This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

With the APT, organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While 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 works in cyber security. 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 cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

Who Should Attend

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



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8570

Keith Palmgren SANS Certified Instructor

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice — responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications.

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Paul A. Henry
▶ GIAC Cert: GCED
▶ Masters Program



SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 36.

“SEC501 offers a great explanation of net defense best practices that are often overlooked.”

-Kirk Glockner, U.S. Navy

“SEC501 is the best technical training course I have ever taken. SEC501 exposed me to many valuable concepts and tools, but also gave me a solid introduction to those tools so that I can continue to study and improve on my own.”

-Curt Smith,

Hidalgo Medical Services



Paul A. Henry SANS Senior Instructor

Paul Henry is a Senior Instructor with the SANS Institute and one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia.



Cybersecurity continues to be a critical area for organizations and will continue to increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks will continue to pose a threat to an organization as data become more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Who Should Attend

- ▶ Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- ▶ People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want a broad, advanced coverage of the core areas to protect their systems
- ▶ Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization



www.giac.org



www.sans.edu

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor
▶ GIAC Cert: GCIA
▶ Masters Program
▶ Cyber Guardian
▶ DoDD 8570



Who Should Attend

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

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the **Intrusion Detection In-Depth** course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the “soup to nuts” or bits to bytes to packets to flow of traffic analysis.

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VM-ware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches. A more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an “extra credit” stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to “hit the ground running” once returning to a live environment.



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8570

“SEC503 added additional skills to my knowledge base. I learned a lot more than I originally expected.”

-Robert Strawley, U.S. Army

“Mike has a gift for making a potentially dry subject matter very interesting; excellent teaching and presentation skills.”

-Jennifer Torres, BAH



Mike Poor SANS Senior Instructor

Mike is a founder and senior security analyst for the 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 in 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.

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program

Sat, May 10 - Thu, May 15
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits

Laptop Required

Instructor: Seth Misenar

- ▶ GIAC Cert: GCIH
- ▶ Masters Program
- ▶ Cyber Guardian
- ▶ DoDD 8570



SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 36.

"SEC504 was a great course in all aspects; content, presentation, and instructor. I would really like more courses and opportunities for this training."

-Tom Patterson, Sage Software

"Seth is an amazing instructor. He clearly has a passion for security, evident by his crazy amount of knowledge. His real-world examples relate well to the course content and make it easier to understand."

-Lee Slaughter, F5 Networks



Seth Misenar SANS Certified Instructor

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security through leadership, independent research, and security training. Seth's background includes network 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 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 which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE.

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors and the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, 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



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8570



Securing Windows with the Critical Security Controls

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jason Fossen
► GIAC Cert: GCWN
► Masters Program
► Cyber Guardian

“Windows is everywhere and security is paramount. No matter whether you hate Windows or not, SEC505 is a must.”

-David Ellis,
MS Army National Guard

“It was incredible that we were able to experiment with Direct Access Control labs in SEC505. DAC is a rapidly evolving trend, and now I understand how it works.”

-Lindsay Inger



How can we deal with pass-the-hash attacks, token abuse, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits which lead to malware infections? These are tough problems, but we tackle them in course SEC505.

While forensics and incident response are great for detection and remediation, the goal of this course is to prevent those infections in the first place (after all, first things first). Hacking tools are fun, but having a bunch of hacking tools doesn't help in securing a large Active Directory network against their use. We need different tools to implement security, and these tools have to scale without spending a fortune, such as Group Policy and PowerShell.

Learning PowerShell is probably the single best new skill for the careers of Windows administrators, especially with the trend towards cloud computing. Because most of your competition lacks scripting skills, it's a great way to make your resume stand out. This course devotes an entire day to PowerShell, but you don't need any prior scripting experience, we'll start with the basics.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows security expertise. The GCWN certification counts towards getting a Master's Degree in information security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8570 computing environment (CE) requirement too.

This is a fun course and a real eye-opener even for Windows administrators with years of experience.



Who Should Attend

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the 20 Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- Anyone who needs to prevent malware infections



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian

Jason Fossen SANS Faculty Fellow

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS' week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS' projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas.

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Timothy Tomes
► GIAC Cert: GWAPT
► Masters Program
► Cyber Guardian

SANS



Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate

to advanced level class, you'll learn the art of exploiting web applications so you can find flaws in your enterprise's web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's web applications to find some of the most common and damaging Web application vulnerabilities today.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

Who Should Attend

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

"SEC542 is an essential course for application security professionals."

-John Yamich, Exact Target

"Web apps assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."

-James Kelly, Blue Canopy LLP

"With the infinite tools used for web application penetration, SEC542 helps you understand and use the best tools for your environment."

-Linh Sithihao, UT South Western Medical Center



Timothy Tomes SANS Instructor

Tim Tomes is a Senior Security Consultant and Researcher for Black Hills Information Security with experience in information technology and application development. A veteran, Tim spent nine years as an Officer in the United States Army conducting various information security related activities. Tim manages multiple open source projects such as the Recon-ng Framework, the HoneyBadger Geolocation Framework, and PushPin, is a SANS Instructor for SEC542 Web Application Penetration Testing, writes technical articles for PaulDotCom, and frequently presents at information security conferences such as ShmooCon and DerbyCon.



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian

Network Penetration Testing and Ethical Hacking

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Ed Skoudis
► GIAC Cert: GPEN
► Masters Program
► Cyber Guardian

“Phenomenal speaking skills, Ed! Very engaging, excellent explanations and examples!”

-Travis Farral,
XTO Energy/ExxonMobile

“Ed Skoudis successfully combines expertise, real-world experiences, and even humor to deliver an incredibly effective learning experience!”

-George Huang,
Nationwide Insurance



Ed Skoudis SANS Faculty Fellow

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing.

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. **SANS SEC560: Network Penetration Testing and Ethical Hacking** truly prepares you to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course.

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then, we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective.

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian

Implementing and Auditing the Twenty Critical Security Controls - In-Depth

Five-Day Program
Sat, May 10 - Wed, May 14
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: James Tarala

SANS

“SEC566 was an outstanding course. The structure and labs very effectively conveyed the concepts, priorities, and implementation of the critical controls. James is an exceptional instructor, and used numerous real-life experiences to illustrate the controls (or lack thereof) which helped make the course content very relevant.”

-James Mitchell,
Mission Support Alliance, LLC



James Tarala SANS Senior Instructor

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with 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 in their security management, operational practices, and regulatory compliance issues, 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.

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 Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British governments 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.

Who Should Attend

- ▶ Information assurance auditors
- ▶ System implementers or administrators
- ▶ Network security engineers
- ▶ IT administrators
- ▶ Department of Defense (DoD) 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
- ▶ Alumni of SEC440, SEC401, SEC501, MGT512, and other SANS Audit courses

Mobile Device Security and Ethical Hacking

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley
▶ GIAC Cert: GMOB
▶ Masters Program

“Superb course! I have taken mobile security courses in the past from other highly reputable companies. However, those courses failed in comparison with the SANS course both in terms of content and in terms of the level of the competency in the instructor.”

-Mark Geeslin, Citrix



www.giac.org



www.sans.edu



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. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GMOB, GPEN, GREM, 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.

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as 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 ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast 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.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

Who Should Attend

- ▶ Penetration testers
- ▶ Ethical hackers
- ▶ Auditors who need to build deeper technical skills
- ▶ Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Larry Pesce
► GIAC Cert: GAWN
► Masters Program
► Cyber Guardian

"SEC617 was great and I am still impressed with the consistency from day 1 - 6. Pesce kept a high level of energy and knowledge throughout."

-Philip Mein, JCCC

"Past experience with SANS has proved & continues to prove their superiority."

-Michael Hennick



Larry Pesce SANS Certified Instructor

Larry is a Senior Security Analyst with InGuardians after a long stint in security and disaster recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties, and his second Leatherman Multi-tool. Larry also co-authored "Linksys WRT54G Ultimate Hacking and Using Wireshark" and "Ethereal" from Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge.

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, but it is growing in deployment and utilization with wireless LAN technology and WiFi as well as with 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 their own set of security challenges and attacker opportunities.

To be a wireless security expert, you need to have a comprehensive understanding of the technology, the threats, the exploits, and the defense 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/TLS, and other systems, including developing attack techniques leveraging Windows 7 and Mac OS X. We'll also 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.

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.



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



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian

Advanced Exploit Development for Penetration Testers

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jake Williams



You Will Learn

- ▶ How to write modern exploits against the Windows 7 and 8 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

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, they could expose organizations to significant attacks, undermining their defenses when wielded by very skilled attackers. 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-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

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

You Will Be Able To

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



Jake Williams SANS Certified Instructor

Jake Williams is a technical analyst with the Department of Defense (DoD) where he has over a decade of experience in systems engineering, computer security, forensics, and malware analysis. Jake has been providing technical instruction for years, primarily with HBGary, where he was the principal courseware developer and instructor for their products. He also maintains malware reverse engineering courses for CSRG Group Computer Security Consultants. Recently, he has been researching the application of digital forensic techniques to public and private cloud environments. Jake has been involved in numerous incident response events with industry partners in various consulting roles. Jake led the winning government team for the 2011 and 2012 DC3 Digital Forensics Challenge. He has spoken at numerous events, including the ISSA events, SANS@Night, the DC3 conference, Shmoocon, and Blackhat. Jake holds a Bachelor's degree in CIS, a Master's Degree in Information Assurance, and is currently pursuing a PhD in Computer Science. His research interests include protocol analysis, binary analysis, malware RE methods, and methods for identifying malware Command and Control (C2) techniques. He holds numerous certifications, including GREM, GCFE, GSNA, GCIA, GCII, GCWN, GPEN, RHCSA, and CISSP.

Computer Forensic Investigations – Windows In-Depth

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Chad Tilbury
► GIAC Cert: GCCE
► Masters Program



Digital Forensics and
Incident Response
<http://computer-forensics.sans.org>

"I really appreciate the prebuilt and configured SIFT workstation. FOR408 course materials and instructions were outstanding."

-Clint Modesitt,
HSSK Forensics, Inc.

"Great forensics info from a technical perspective in terms of theory, tools, and processes. A great way to get started! FOR408 also has good info for the seasoned forensics analyst; you won't be disappointed!"

-Jonathan Stidham, Raytheon



Chad Tilbury SANS Certified Instructor

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics.

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threats, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and an calling cybercrime law enforcement agents to piece together what happened in these cases.

Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

FOR408: Computer Forensic Investigations – Windows In-Depth focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 8 and Server 2008) you will be exposed to well known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer; FTK Imager; Prefetch Analyzer; and much more. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that students can take with them.



www.giac.org



www.sans.edu

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

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Rob Lee
► GIAC Cert: GCFA
► Masters Program
► Cyber Guardian
► DoDD 8570



Digital Forensics and
Incident Response
<http://computer-forensics.sans.org>

What you will receive with this course

- SIFT Workstation Virtual Machine
- F-Response TACTICAL Edition with a 2 year license
- Best-selling book "File System Forensic Analysis" by Brian Carrier
- Course DVD loaded with case examples, additional tools, and documentation

"FOR508 is fantastic; a roller coaster barrage of forensic tools and nuances backed by real-world scenarios."

-Razi Asaduddin, ExxonMobil



Rob Lee SANS Faculty Fellow

Rob Lee is an entrepreneur and consultant in the Washington D.C. area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response.

Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led crime investigations and an incident response team. Over the next 7 years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book "Know Your Enemy, 2nd Edition." Rob is also co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat.

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT — the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

FOR508 will help you determine:

- **How did the breach occur?**
- **What systems were compromised?**
- **What did they take? What did they change?**
- **How do we remediate the incident?**

This course trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

Who Should Attend

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates



www.giac.org



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8570

Advanced Network Forensics and Analysis

Six-Day Program

Sat, May 10 - Thu, May 15

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Philip Hagen



SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 36.



Digital Forensics and Incident Response
<http://computer-forensics.sans.org>

What you will receive with this course

- Linux version of the SIFT Workstation Virtual Machine with over 500 digital forensics and incident response tools prebuilt into the environment, including network forensic tools added just for this course
- Windows Virtual Machine with preinstalled network forensic tools
- Windows 8 Standard Full Version License and Key for the Windows VMware Image
- Realistic case data to examine during class, from multiple sources
- 64GB USB disk loaded with case examples, tools, and documentation



Philip Hagen SANS Instructor

Philip Hagen has over 14 years of experience in creating and deploying strategic and ad-hoc IT and infosec solutions. He has managed small, tactical projects and large government contracts. Phil started his security career while attending the US Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a Communications Officer, and was assigned to a base-level Year 2000 project management office. The plans he helped create were later used during California's rolling power blackouts. At the Pentagon, he later managed a support team serving 200 analysts. In 2003, Phil shifted to a government contractor, providing technical services for exotic IT security projects. These included systems that demanded 24x7x365 functionality. He supported the design, deployment, and support of a specialized network for 100 security engineers in ten offices. He later managed a team of 85 computer forensic professionals in the National Security sector. Most recently, Phil formed Lewes Technology Consulting, LLC. He applies his IT and security experience to small and medium businesses as they track toward their business goals, and performs forensic casework and infosec training.

NEW

SANS

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

Who Should Attend

- ▶ Incident response team members
- ▶ Law enforcement officers, federal agents, and detectives
- ▶ Information security managers
- ▶ Network defenders
- ▶ IT professionals
- ▶ Network engineers
- ▶ IT lawyers and paralegals
- ▶ Anyone interested in computer network intrusions and investigations

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 necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap 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.

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.

Advanced Smartphone Forensics

NEW

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Heather Mahalik



Digital Forensics and
Incident Response
<http://computer-forensics.sans.org>

What you will receive with this course

- SIFT Workstation Smartphone Version Windows Virtual Machine used with all class hands-on exercises. The workstation is used to teach digital forensic examiners and incident responders how to examine and investigate information on smartphones. SIFT contains free and open source tools, easily matching any modern forensic tool suite.
- Windows 8 Standard License
- Oxygen Forensic Educational License
- Microsystemation XRY Demo License
- Cellebrite Physical Analyzer Demo License
- Course USB loaded with case examples, exercises, and documentation



Heather Mahalik, SANS Certified Instructor

Heather Mahalik is a senior digital forensics analyst at Basis Technology. As the on-site project manager, she uses her experience to manage the cell phone exploitation team and supports media and cell phone forensics efforts in the U.S. government. Heather has worked in digital forensics for over ten years and has performed thousands of forensic acquisitions and examinations on hard drives, e-mail and file servers, mobile devices, and portable media. Previously, Heather worked as a forensic examiner for Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high profiles cases. She has authored papers, presented at leading conferences, and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather's background is based on media forensics, and she currently specializes in BlackBerry, Nokia, knock-off, Android, and iOS Forensics.

It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individual's movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

FOR585: Advanced Smartphone Forensics focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner; understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. FOR585, originally conceptualized by Eoghan Casey, Heather Mahalik and Terrance Maguire, addresses today's smartphone technologies and threats by studying real-life investigative scenarios. ***Dont miss the NEW FOR585!***

The hands-on exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones. This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensic professionals. ***Its time to get smarter!***

Who Should Attend

- ▶ Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- ▶ Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and files they accessed
- ▶ Information security professionals who respond to data breach incidents and intrusions
- ▶ Incident response teams tasked with identifying the role that smartphones played in a breach
- ▶ Law enforcement officers, federal agents, or detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- ▶ IT auditors who want to learn how smartphones can expose sensitive information.
- ▶ SANS SEC575, FOR563, FOR408, and FOR508 graduates looking to take their skills to the next level



Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program
Sat, May 10 - Thu, May 15
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Lenny Zeltser
► GIAC Cert: GREM
► Masters Program



Digital Forensics and
Incident Response
<http://computer-forensics.sans.org>

**"FOR610 is
incredibly useful
and comprehensive,
from start to finish."**

-Jon Poling, Dell Secure

**"Lenny taught in a
way that made tough
topics very clear for
me. I have had a lot
of "aha" moments and
I am excited!"**

-Eylia McCastle,
Booz Allen Hamilton



www.giac.org



www.sans.edu



Lenny Zeltser SANS Senior Instructor

Lenny Zeltser is a seasoned business leader with extensive experience in information technology and security. As a product management director at NCR Corporation, he focuses on safeguarding IT infrastructure of small and midsize businesses world-wide. Before NCR,

Lenny led the enterprise security consulting practice at a major IT hosting provider. In addition, Lenny is a Board of Directors member at SANS Technology Institute and a volunteer incident handler at the Internet Storm Center. Lenny's expertise is strongest at the intersection of business, technology and information security practices and includes incident response, cloud services and product management. He frequently speaks at conferences, writes articles and has co-authored books on network security and malicious software defenses. Lenny is one of the few individuals in the world who've earned the prestigious GIAC Security Expert designation. He has an MBA degree from MIT Sloan and a Computer Science degree from the University of Pennsylvania.

Who Should Attend

- Professionals with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration
- Professionals who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs
- Individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their malware forensics expertise

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs—spyware, bots, trojans, etc.—that target or run on Microsoft Windows. This training also looks at reversing web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

The course begins by covering fundamental aspects of malware analysis and continues by discussing essential x86 assembly language concepts. Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware.

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss malware analysis tools and techniques of intermediate complexity. Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops, and functions. The course spends some time discussing essential aspects of x86 assembly to allow malware analysts to navigate through malicious executables using a debugger and a disassembler.

SANS® +S™ Training Program for the CISSP® Certification Exam

Six-Day Program

Sat, May 10 - Thu, May 15

9:00am - 7:00pm (Day 1)

8:00am - 7:00pm (Days 2-5)

8:00am - 5:00pm (Day 6)

46 CPE/CMU Credits

Laptop NOT Needed

Instructor: Eric Conrad

► GIAC Cert: GISP

► DoDD 8570

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

www.sans.org/special/cissp-get-certified-program

“Eric’s style of teaching captivates his students; his use of stories and real-life scenarios drive home the learning. MGT414 is by far the most effective training that I have had.”

-Neel Sehgal, Honeywell Int’l.

“MGT414 is simply the best way to prepare for the CISSP. Great test taking tips, relevant examples, and real-life meaningful illustrations.”

-Thomas Cook, USMA



Who Should Attend

- Security professionals who are interested in understanding the concepts covered in 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® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

- Domain 1: Access Controls
- Domain 2: Telecommunications and Network Security
- Domain 3: Information Security Governance & Risk Management
- Domain 4: Software Development Security
- Domain 5: Cryptography
- Domain 6: Security Architecture and Design
- Domain 7: Security Operations
- Domain 8: Business Continuity and Disaster Recovery Planning
- Domain 9: Legal, Regulations, Investigations and Compliance
- Domain 10: Physical (Environmental) Security



www.giac.org



www.sans.org/8570

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of 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

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.



Eric Conrad SANS Certified Instructor

Eric Conrad is lead author of the book “The 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 president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, 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.

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program

Sat, May 10 - Wed, May 14

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPE/CMU Credits

Laptop NOT Needed

Instructor: G. Mark Hardy

► GIAC Cert: GSLC

► Masters Program

► doDD 8570

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 gain 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 US 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, 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™

Knowledge Compression™ is an optional add-on feature to a SANS class which 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!

Who Should Attend

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

"MGT512 encompasses topics in all security areas. This was my first SANS experience and I greatly enjoyed it. I will certainly advocate to my superiors the value I have received."

-Mark McCready,
Modern Woodmen of America

"MGT512 course material and the instructor were top notch. SANS delivers a quality product every time."

-Charles Brown III,
MCSF-Blount Island



www.giac.org



www.sans.edu



www.sans.org/8570



G. Mark Hardy SANS Certified Instructor

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security 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. G. Mark 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 US 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.

Auditing Networks, Perimeters, and Systems

Six-Day Program

Sat, May 10 - Thu, May 15

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: David Hoelzer

▶ GIAC Cert: GSNA

▶ Masters Program

▶ DoDD 8570

"AUD507 is excellent, I could not have spent the cost of the course any better!"

-Johnson Gathumbi,
Inova Health System

"In 20+ years of industry experience, I have never seen a smoother intro to batch progress to branching and looping. Well done!"

-Michael Decker, CNS Security



David Hoelzer SANS Faculty Fellow

David Hoelzer is a high-scoring SANS Fellow instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow in the Center for Cybermedia Research and also a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.

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 organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, 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 will be given from real-world examples.

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. 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 how to automatically validate defenses through instrumentation and automation of audit checklists.

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 experience the mix of theoretical, hands-on, and practical knowledge.

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 they 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



www.giac.org



www.sans.edu



www.sans.org/8570

AUD444 Auditing Security and Controls of Active Directory and Windows

Three-Day Course
Sat, May 10 - Mon, May 12
9:00am - 5:00pm
18 CPE/CMU Credits
Instructor: Bryan Simon

Who Should Attend

- ▶ Internal auditors
- ▶ IT specialist auditors
- ▶ IT auditors
- ▶ IT audit managers
- ▶ Information system auditors
- ▶ Information security officers

"AUD444 offers relevant theory backed by experience and great hands-on practice."

-Bryan Camereno,
Charles Schwab

Auditors need to be able to understand how Active Directory operates and the key business risks that are present. This course was written to teach auditors how to identify and assess those business risks. Active Directory and Windows systems are typically well known and utilized within organizational infrastructures. However, they can be difficult to audit since there are a large number of settings on the end system. This course provides the tools and techniques to effectively conduct an Active Directory and Windows audit, and while doing so identify key business process controls that may be missing. Students have the opportunity to look at the business process controls and then how those can be verified by looking at Active Directory and the Windows systems that exist. Plus, students are taught how to add additional value to their audits by being able to identify the technology risks that may have been overlooked. The hands-on exercises reinforce the topics discussed in order to give students the opportunity to conduct an audit on their own Windows systems, as well as understand the different security options that Windows provides.



Bryan Simon SANS Instructor

Bryan Simon is a cybersecurity professional, and an instructor at the SANS Institute. Bryan has 23 years of experience in operational IT, and has specialized in IT security for the past 13 years. 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 national conferences and with the press on matters of cybersecurity. Bryan has specialized expertise in vulnerability assessments, penetration testing, and auditing. Bryan has received recognition for his work in IT security, and was most recently profiled by McAfee as an IT Hero. Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program.

AUD445 Auditing Security and Controls of Oracle Databases

Three-Day Course
Tue, May 13 - Thu, May 15
9:00am - 5:00pm
18 CPE/CMU Credits
Instructor: Bryan Simon

Who Should Attend

- ▶ Internal auditors
- ▶ IT specialist auditors
- ▶ IT auditors
- ▶ IT audit managers
- ▶ Information system auditors
- ▶ Information security officers

"AUD445 covers the important knowledge needed to perform an effective Oracle database audit."

-Gary Johnson,
Colorado PERA

Over the past few years we have seen attackers target data since there is a financial incentive to being able to compromise valuable data. The media seems to be reporting new data compromises constantly. That means auditors need to be effectively auditing the controls that should exist to protect this valuable organizational asset.

Oracle Databases often store the data that's being targeted. Oracle Databases are very complex and challenging to audit! Auditors need to be able to effectively audit the processes and controls in place around the database to ensure the asset is being properly protected and the risks properly managed.

This course provides all of the details, including the IT process, procedural and technical controls, that you as an auditor should look for when conducting an Oracle database audit. Even better, you have the opportunity to get firsthand experience extracting and interpreting data from a live Oracle Database which allows you to be able to return and immediately conduct an Oracle Database audit. By getting hands-on experience, you get a better understanding of exactly how an Oracle Database operates and what data is available for audit purposes. The course is also put together in such a way that you can add additional value to the business and provide further security recommendations and benefits for the database being audited.

SEC434 Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting

Two-Day Course

Thu, May 8 - Fri, May 9

9:00am - 5:00pm

12 CPE/CMU Credits

Instructor: Jake Williams

Bio on page 13

This first-ever dedicated log management class teaches system, network, and security logs, their analysis and management and covers the complete lifecycle of dealing with logs: the whys, how's and whats.

You will learn how to enable logging and then how to deal with the resulting data deluge by managing data retention, analyzing data using search, filtering and correlation as well as how to apply what you

learned to key business and security problems. The class also teaches applications of logging to forensics, incident response and regulatory compliance.

In the beginning, you will learn what to do with various log types and provide brief configuration guidance for common information systems. Next, you will learn a phased approach to implementing a company-wide log management program, and go into specific log-related tasks that needs to be done on a daily, weekly, and monthly basis in regards to log review and monitoring.

Everyone is looking for a path through the PCI DSS and other regulatory compliance maze and that is what you will learn in the next section of the course. Logs are essential for resolving compliance challenges; this class will teach you what you need to concentrate on and how to make your log management compliance-friendly. And people who are already using log management for compliance will learn how to expand the benefits of your log management tools beyond compliance.

You will learn to leverage logs for critical tasks related to incident response, forensics, and operational monitoring. Logs provide one of the key information sources while responding to an incident and this class will teach you how to utilize various log types in the frenzy of an incident investigation.

The class also includes an in-depth look at deploying, configuring and operating an open source tool OSSEC for log analysis, alerting and event correlation.



SEC524 Cloud Security Fundamentals

Two-Day Course

Thu, May 8 - Fri, May 9

9:00am - 5:00pm

12 CPE/CMU Credits

Instructor: Paul A. Henry

Bio on page 4

The SANS Cloud Security Fundamentals course starts out with a detailed introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types including: public, private, and hybrid.

An overview of security issues within each of these models will be covered with in-depth discussions of risks to consider. Attendees will go in-depth on architecture and infrastructure fundamentals for private, public, and hybrid clouds. A wide range of topics will be covered including: patch and configuration management, virtualization security, application security, and change management. Policy, risk assessment, and governance within cloud environments will be covered with recommendations for both internal policies and contract provisions to consider. This path leads to a discussion of compliance and legal concerns. The first day will wrap-up with several fundamental scenarios for students to evaluate.

Attendees will start off the second day with coverage of audits and assessments for cloud environments. The day will include hands-on exercises for students to learn about new models and approaches for performing assessments, as well as evaluating audit and monitoring controls. Next the class will turn to protecting the data itself! New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in-depth. The challenges of identity and access management in cloud environments will be covered. The course will move into disaster recovery and business continuity planning using cloud models and architecture. Intrusion detection and incident response in cloud environments will be covered along with how best to manage these critical security processes and technologies that support them given that most controls are managed by the CSP.

SEC546 IPv6 Essentials

Two-Day Course

Fri, May 16 - Sat, May 17

9:00am - 5:00pm

12 CPE/CMU Credits

Instructor: Dr. Johannes Ullrich

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 over the next years to grow, in particular as mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn

how to detect IPv6 and defend against threats unintentional IPv6 use may bring.

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more and more important to global commerce.

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course

Fri, May 16 - Sat, May 17

9:00am - 5:00pm

12 CPE/CMU Credits

Instructor: Eric Conrad

Bio on page 19

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.



MGT305 Technical Communication and Presentation Skills for Security Professionals

One-Day Course

Fri, May 9

9:00am - 5:00pm

6 CPE/CMU Credits

Instructor: David Hoelzer

Bio on page 21

► Masters Program



www.sans.edu

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, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Attendees will also get a crash course on advanced public speaking skills

Professionals like you have come to expect the very best in materials and presentation quality from SANS courses. In this course we have distilled the elements that go into writing high-quality material and the skills required to be a top public speaker from nearly two decades of experience. For years students have asked for a course on writing and delivering presentations; this course is the answer!

MGT415 A Practical Introduction to Risk Assessment

NEW

One-Day Course

Fri, May 9

9:00am - 5:00pm

6 CPE/CMU Credits

Instructor: James Tarala

Bio on page 10

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 that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their 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

Thu, May 8 - Fri, May 9

9:00am - 5:00pm

12 CPE/CMU Credits

Instructor: Lance Spitzner

► Masters Program



SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 36.

Organizations have invested a tremendous amount of money and resources into securing technology, but little, if anything, into securing the human element. As a result, people are now the weakest link; the simplest way for cyber attackers to hack into any organization is to target your employees. One of the most effective ways to secure the human element is to build an active awareness and education program that goes beyond just compliance and changes behaviors. In this challenging course you will learn how to do just that. You will learn the key concepts and skills needed to build, maintain and measure a high-impact security awareness program. All course content is based on lessons learned from hundreds of organizations around the world. In addition, you will learn not only from extensive interaction with the instructor, but from working with your peers, as well. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so that you can immediately implement your own customized awareness program upon returning to your organization.



www.sans.edu



Lance Spitzner SANS Certified Instructor

Lance Spitzner is an internationally recognized leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books, and has published over thirty security whitepapers. Mr. Spitzner started his security career with Sun Microsystems as a senior security architect, helping secure Sun's customers around the world. He is founder of the Honeynet Project; an international, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public.

BONUS SESSIONS

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given 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.

EMERGING TRENDS

KEYNOTE: **Emerging Security Trends: Crossing the Chasm to Protecting a “Choose Your Own IT” World**

John Pescatore

Threats are mutating constantly, and users are demanding to use more devices and more cloud services. John Pescatore will give a data-driven presentation on the recent and future trends in advanced threats, and he will highlight the evolutions (and some revolution) needed in security processes, architecture, and technology in order to protect the business in 2014 and beyond. Take home new ideas and guidance for targeting the knowledge you'll gain at SANS Security West at the highest payback security challenges.

EMERGING TRENDS

Will The Real Next-Generation Security Please Stand Up?

Moderator: John Pescatore

At Gartner in 2003, John Pescatore first published the phrase “Next-Generation Firewall.” As punishment for that, he will moderate a panel of SANS and industry experts discussing what is real and what is hype about security solutions for dealing with advanced targeted threats and changes in how IT is delivered and consumed. Come prepared to join in a lively discussion.

EMERGING TRENDS

Offense Informs Defense *Moderators: Ed Skoudis & Mike Poor*

Ed Skoudis, Mike Poor, and a panel of SANS Pen Testing and SANS Cyber Defense faculty will discuss the top Emerging Trends predicted by Security West 2014 students.

*Tweet your Emerging Trend predictions to **#SecWestTrends** or visit **www.SANS.org/SecWest-Trends***

EMERGING TRENDS

Emerging Trends in DFIR *Moderator: Rob Lee*

Rob Lee and a panel of SANS DFIR faculty will discuss the top Emerging Trends in DFIR predicted by Security West 2014 students.

*Tweet your Emerging Trend predictions to **#SecWestTrends** or visit **www.SANS.org/SecWest-Trends***

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 Seth Misenar and Eric Conrads new course: Continuous Monitoring and Security Operations.

An Introduction to PowerShell for Security Assessments

James Tarala

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone all in with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of these Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

Evolving Threats *Paul A. Henry*

For nearly two decades defenders have fallen into the “Crowd Mentality Trap” and have simply settled on doing the same thing everyone else was doing while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers’ delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and \$157 billion (USD) in data breach costs in only the past 6 years.

Securing The Kids *Lance Spitzner*

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top five steps you can take to protect them. This talk is based on the experiences and lessons learned from a variety of SANS top instructors who not only specialize in security, but are parents just like you. This talk is sponsored and delivered by SANS Securing The Human program.

Effective Phishing that Employees Like *Lance Spitzner*

One of the toughest challenges in establishing a high-impact security awareness program is measuring the impact. Are you changing behavior and reducing risk? Phishing assessments are a powerful way to measure such change, while addressing one of the most common human risks. As more organizations use phishing assessments, many of them are doing it wrong, not only negatively impacting their metrics but generating resentment among employees. In this short presentation, learn how to create a fun, engaging phishing program that not only effectively measures and reinforces key behaviors, but is also truly enjoyed by employees.

The State of Eavesdropping on Cellular Networks *Christopher Crowley*

Security research in the 3G and 4G network space is restricted due to legal issues in the United States. Christopher Crowley will discuss the current known, open source information related to known cellular attacks. He will also discuss the attack methodology associated with cellular client duping, a strategy for convincing a cellular device to connect to an attacker controlled cell tower.

The 13 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified thirteen “Absolute Truths” of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

How the West was Pwned *G. Mark Hardy*

Can you hear it? The giant sucking sound to the East? With it are going more than just manufacturing jobs — it’s our manufacturing know-how, intellectual property, military secrets, and just about anything you can think of. If we’re so technologically advanced, how are the People’s Republic of China (PRC) and others able to continue to pull this off? Why do we keep getting pwned at our own game? The Mandiant APT1 report released last year detailed research into People’s Liberation Army (PLA) Unit 61398 and their significant penetration into western networks. It was followed quickly by a series of political and diplomatic statements denouncing China’s actions, which China flatly denied. Where’s the truth? We’ll try to find it. There’s a lot of talk about cyber war, but there may not be a war. If a victor can extract tribute from the vanquished, war isn’t necessary. Today, intellectual capital is a proxy for tribute. We’ll look at some specifics about what operations have been run against us and progress in efforts to create an international legal framework for cyberwar in case the bits start flying.

Vendor Solutions Expo

Monday, May 12 | 10:30am-10:50am | 12:30pm-1:15pm | 3:00pm-3:20pm

Our events incorporate external vendor partners showcasing some of the best security solutions available. Take advantage of the opportunity to interact with the people behind the products and learn what they have to offer you and your organization.

The Core NetWars Tournament and the DFIR NetWars Tournament will be held simultaneously at Security West 2014!

CORE NETWARS TOURNAMENT

NETWARS

A True Hands-On Interactive Security Challenge!



Core NetWars

NetWars 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 bases are using NetWars OnSites to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

Who Should Attend

- ▶ **Security professionals**
- ▶ **System administrators**
- ▶ **Network administrators**
- ▶ **Ethical hackers**
- ▶ **Penetration testers**
- ▶ **Incident handlers**
- ▶ **Security auditors**
- ▶ **Vulnerability assessment personnel**
- ▶ **Security Operations Center (SOC) staff members**

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

**Both NetWars
competitions
will be played
over two evenings:
May 13-14, 2014**

Prizes will be awarded at the
conclusion of the games.
**REGISTRATION IS LIMITED
AND IS FREE**
for students attending any
long course at Security West 2014
(NON-STUDENTS ENTRANCE FEE
IS \$1,249).

Register at www.sans.org/event/sans-security-west-2014/courses

DFIR NetWars

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges. DFIR NetWars Tournament is packed with challenges covering host forensics, network forensics, and malware and memory analysis. It is 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.

Who Should Attend

- ▶ **Digital forensic analysts**
- ▶ **Forensic examiners**
- ▶ **Reverse engineering and malware analysts**
- ▶ **Incident responders**
- ▶ **Law enforcement officers, federal agents, or detectives**
- ▶ **Security Operations Center (SOC) analysts**
- ▶ **Cyber crime investigators**
- ▶ **Media exploitation analysts**

**Challenge yourself
before the enemy does –
DFIR NetWars**



Best of the best! Winners of the most recent NetWars Tournament of Champions held at SANS CDI 2013.

How Are You Protecting Your

- **Data?**
- **Network?**
- **Systems?**
- **Critical Infrastructure?**

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification.

Get GIAC certified!

GIAC offers over 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.



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

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

Get Certified at

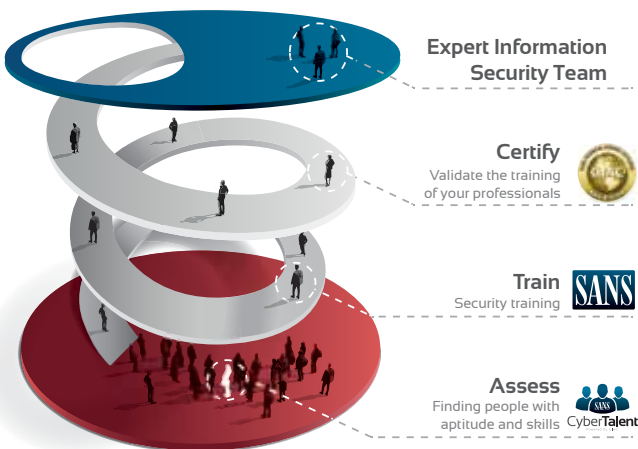
www.giac.org



Contact Us to Learn More
www.sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

Introducing SANS CyberTalent Assessments, a new web-based recruitment and talent management tool that helps validate the skills of information security professionals. This unique tool may be used during the recruitment process of new information security employees and to assess the skills of your current staff to create a professional development plan. This tool will save you money and time, as well as provide you with the information required to ensure you have the right skills on your information security team.



Benefits of SANS CyberTalent Assessments

For Recruiting

- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

For Talent Management

- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps develop a professional development plan

US and Canada 301.654.SANS (7267)

EMEA and APAC inquiries: + 44 (0) 20 3598 2363



SANS

CYBER GUARDIAN

PROGRAM

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.

Real Threats

Real Skills

Real Success

Join Today!

Contact us at
onsite@sans.org
to get started!

[www.sans.org/
cyber-guardian](http://www.sans.org/cyber-guardian)

Prerequisites

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

Core Courses

SEC503 (GCIA) | SEC504 (GCIH) | SEC560 (GPEN) | FOR508 (GCFA)

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

Blue Team Courses

SEC502 (GPPA) | SEC505 (GCWN) | SEC506 (GCUX)

Red Team Courses

SEC542 (GWAPT) | SEC617 (GAWN) | SEC660 (GXPN)

Department of Defense Directive 8570 (DoDD 8570)

www.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.

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 Techniques, Exploits, and Incident Handling	GCIH
AUD507 Auditing Networks, Perimeters, and Systems	GSNA
FOR508 Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512 SANS Security Essentials for Managers with Knowledge Compression™	GSLC

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

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 www.sans.org/8570

WHAT'S YOUR NEXT CAREER MOVE?

SANS Technology Institute, an independent subsidiary of SANS, is now accredited by The Middle States Commission on Higher Education!

3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

"It's great to learn from an organization at the forefront of both academics, and in the field."

-JOSEPH FAUST,
MSISE PROGRAM

Two unique, respected master's degree programs:

**MASTER OF SCIENCE IN
INFORMATION SECURITY ENGINEERING**

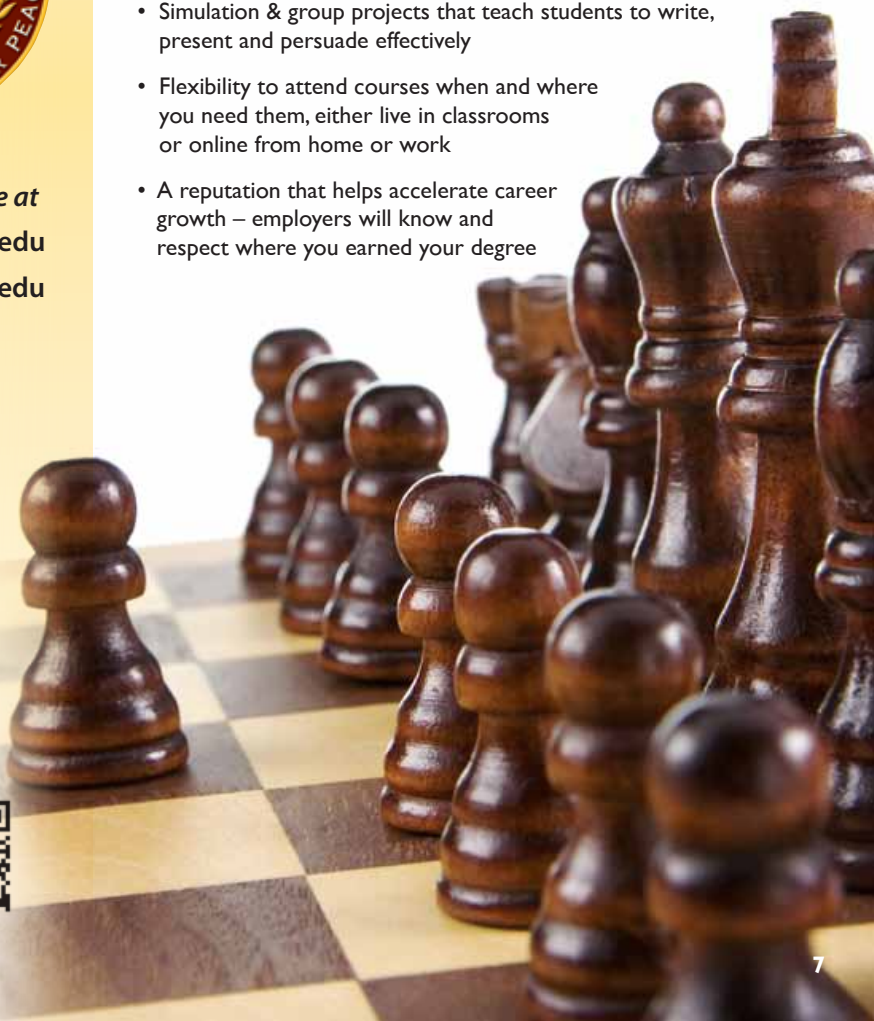
**MASTER OF SCIENCE IN
INFORMATION SECURITY MANAGEMENT**

SANS Technology Institute offers key qualities students seek in a cyber master's program:

- World-class, cutting-edge technical courses that establish and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership,
- Simulation & group projects that teach students to write, present and persuade effectively
- Flexibility to attend courses when and where you need them, either live in classrooms or online from home or work
- A reputation that helps accelerate career growth – employers will know and respect where you earned your degree



Learn more at
www.sans.edu
info@sans.edu



SECURING THE HUMAN

SECURITY AWARENESS FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of modules:
 - STH.End User is mapped against the Critical Security Controls.
 - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
 - STH.Utility fully addresses NERC-CIP compliance.
 - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
 - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.



For a free trial visit us at:
www.securingthehuman.org

FUTURE SANS TRAINING EVENTS

Information on all events can be found at www.sans.org/security-training/by-location/all



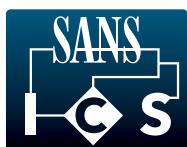
SANS Cyber Guardian 2014

Baltimore, MD | March 3-8

dē-'fər-'kän

SANS DFIRCON 2014

Monterey, CA | March 5-10



Industrial
Control
Systems

ICS Security SUMMIT 2014 - ORLANDO

Lake Buena Vista, FL | March 12-18



SANS Northern Virginia 2014

Reston, VA | March 17-22



SANS 2014

Orlando, FL | April 5-14



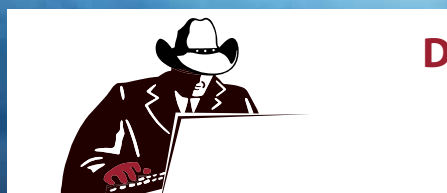
SANS Austin 2014

Austin, TX | April 28 - May 3



Security Leadership SUMMIT 2014

Boston, MA | April 30 - May 7



Digital Forensics & Incident Response SUMMIT

Austin, TX | June 3-10



SANS Rocky Mountain 2014

Denver, CO | June 9-14

FUTURE SANS TRAINING EVENTS

Information on all events can be found at www.sans.org/security-training/by-location/all



SANSFIRE 2014

Baltimore, MD | June 21-30



SANS Capital City 2014

Washington, DC | July 7-12



SANS San Francisco 2014

San Francisco, CA | July 14-19



Industrial
Control
Systems

ICS Security SUMMIT 2014 - HOUSTON

Houston, TX | July 21-25



SANS Boston 2014

Boston, MA | July 28 - August 2



SANS Albuquerque 2014

Albuquerque, NM | September 15-20



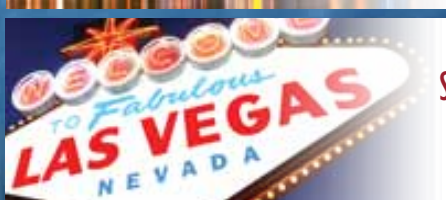
SANS CyberCon Fall 2014

Online | Fall 2014 (TBD)



SANS Baltimore 2014

Baltimore, MD | September 22-27



SANS Network Security 2014

Las Vegas, NV | October 20-25



You don't have to miss out on SANS' top-rated training. Attend select Security West 2014 courses remotely via SANS Simulcast!

How SANS Simulcast Works

Cutting-edge webcast technology and live instruction combine to deliver a fun and engaging remote learning experience. Remote students will also receive four months of access to an archived copy of the class to use as a reference tool or to catch up on a missed session. The platform is web-based so students simply need a solid internet connection to participate.

"This is the first web-based training course I have done and was wondering if it would actually be worthwhile.

It surpassed my expectations! The software and technology worked really well, the presenter kept everything moving along nicely and was quick to pick up on participants' comments during the lecture segments. The IM component adds value — lots of good information/comments from the class."

-Jeremy Gay, Montana State University

The following courses will be available via SANS Simulcast:

SEC401

SEC501

SEC504

FOR572

MGT433

SANS Event Simulcast classes are:

COST-EFFECTIVE — You can save thousands of dollars on travel costs, making Event Simulcast an ideal solution for students working with limited training budgets or travel bans.

ENGAGING — Event Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.

CONDENSED — Complete your course quickly; all SANS Event Simulcast classes take no longer than six days to complete.

REPEATABLE — Event Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.

COMPLETE — You will receive the same books, discs, and MP3 audio files that conference students receive, and you will see and hear the same information as it is presented at the live event.

To register for a SANS Security West 2014 Simulcast course, please visit www.sans.org/event/sans-security-west-2014/attend-remotely



SANS SECURITY WEST 2014

Hotel Information

Training Campus
Manchester Grand Hyatt San Diego

One Market Place
San Diego, CA 92101

www.sans.org/event/sans-security-west-2014/location

Special Hotel Rates Available

A special discounted rate of \$210.00 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 April 19, 2014.

Experience San Diego, California hotel living on a grand scale at Manchester Grand Hyatt San Diego. The best of San Diego is right outside their door. Wake to the sun sparkling off San Diego Bay, indulge in breakfast on the boardwalk at Sally's, then head out to Seaport Village or enjoy a coastal cruise, a walk through the Gaslamp Quarter; a day at San Diego Zoo, SeaWorld, or Balboa Park. Later, look forward to a great night's sleep in their Respire Hypo Allergenic Rooms.

Top 5 reasons to stay at the Manchester Grand Hyatt

- 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 Manchester Grand Hyatt, 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 Manchester Grand Hyatt that you won't want to miss!
- 5 Everything is in one convenient location!

SANS SECURITY WEST 2014

Registration Information

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



Register online at www.sans.org/event/sans-security-west-2014/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.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	3/12/14	\$400.00	3/26/14	\$250.00

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 www.sans.org/security-training/discounts prior to registering.

*Early-bird rates and/or other discounts cannot be combined with the group discount.

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 April 16, 2014 — 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.

www.sans.org/vouchers

EMERGING TRENDS

Panels will discuss the top **Emerging Trends** predicted by Security West 2014 students

**KEYNOTE: Emerging Security Trends:
Crossing the Chasm to Protecting a
“Choose Your Own IT” World**
Moderated by John Pescatore

Emerging Trends: Offense Informs Defense
Moderated by Ed Skoudis & Mike Poor

Emerging Trends in DFIR
Moderated by Rob Lee

Tweet your predictions for
Emerging Trends to
#SecWestTrends

or visit

www.SANS.org/SecWest-Trends



Scan the QR code to register
and pay by March 12th and
SAVE \$400
on Security West courses.

www.sans.org/info/148040