THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Security East 2014

New Orleans, LA | January 20-25

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

Web App Penetration Testing and Ethical Hacking

Reverse-Engineering Malware: Malware Analysis Tools & Techniques

Advanced Computer Forensic Analysis and Incident Response

And more!

"SANS training experience is awesome, and valuable for security professionals and operational teams."

-Ken Langley, UNC School of Medicine

GIAC Approved Training

Register at
www.sans.org/event/security-east-2014

Save $400
by registering early!
See page 17 for more details.

SANS will return to the "Big Easy" for **SANS Security East 2014** on **January 20-25**. Start the new year off right with our top-rated instructors and outstanding course offerings. Now is the time to improve your information security, computer forensics, penetration testing, or IT audit skills.

Our lineup of ten information-packed courses will provide a great training experience. The full list of courses offered in New Orleans can easily be found on the Courses-at-a-Glance section with complete course descriptions and instructor bios on the pages that follow. Also, don't miss our bonus evening presentations and Vendor events where we'll share the latest threats and discuss the best solutions.

Some of the courses at Security East 2014 will also be accepted as credit under the STI Master's degree program. The **SANS Technology Institute** (STI) offers Master's Degree in Information Security Management (MSISM) or Master's Degree in Information Security Engineering (MSISE). Apply by going to the STI homepage (**www.sans.edu**) and clicking the *Learn More* button.

Put the skills you'll learn to practical use and join more than 52,000 GIAC certified professionals who make the cybersecurity industry safe! Visit the GIAC page for more information and register for your certification attempt today.

Our SANS Security East 2014 campus is once again the **Sheraton New Orleans**, in the heart of the Big Easy. The Canal Street location borders the French Quarter, where the city's major attractions and the Mississippi River are literally right outside the hotel's door. Close to the Sheraton you can tour the Mississippi, walk Bourbon Street, visit a plantation, shop at Riverwalk Marketplace or Canal Place, take a swamp tour, see the Aquarium of the Americas, and learn about New Orleans' rich and unique history. This city is a fabulous destination with something of interest for everyone! A special discounted rate of $189 S/D will be honored based on space availability through December 27.

Join us in New Orleans for the best security training your money can buy. Valuable professional relationships that last for years are forged at SANS events, and excellent networking opportunities will be available to you at SANS Security East 2014. What makes SANS courses the best investment for information security training? They are full of important and immediately useful techniques that you can put to work as soon as you return to your office. That is the SANS Promise!

You won't want to miss SANS Security East 2014 where you can experience the very best security training. ***Register and pay by Wednesday, November 27, to receive a $400.00 discount.*** Start making your training and travel plans now and let your colleagues and friends know about SANS Security East 2014. We look forward to seeing you there!

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

"I had a great time. SEC560 has tons of useful material and techniques. As with all SANS training, I leave knowing that I can apply this as soon as I'm back at work."
-Benjamin Bagby, XE.Com

"Couldn't have received such detailed hands-on material anywhere else. Keep up the good work."
-Saubhik Datta, C-DAC

"SANS has excellent variety and quality courses. Excellent reputation."
-Joshua Rose, Geisinger Health System

"Great add-ins and demos. By far the best professional training I have ever received."
-Reggie Hendrick, SRL

Courses-at-a-Glance

SECURITY 301

Intro to Information Security

Course updated to include hands-on labs!

SANS

Five-Day Program
Mon, Jan 20 - Fri, Jan 24
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Fred Kerby
▸ GIAC Cert: GISF

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.

Who Should Attend

- Persons new to information technology who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and information security officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

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.

GISF
www.giac.org

"I like that SEC301 coursework included examples that required us to apply the material in a more real life situation."
-Christa Hedman, Isle of Capri Casinos, Inc.

"SEC301 was the perfect training for me. I've just moved from an executive assistant role in information security to an analyst role and needed to get a solid foundation. This course is giving me the fundamentals."
-Tristan Mahan, Key Bank

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.

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Dr. Eric Cole

- 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 11.

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. 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.

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, 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

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.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian


www.sans.org/8570

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including "Hackers Beware," "Hiding in Plain Site," "Network Security Bible," and "Insider Threat." He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. He is a SANS faculty Fellow and course author.

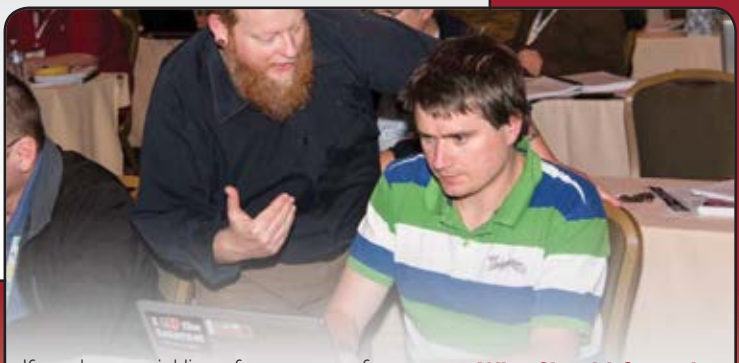
SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor

- GIAC Cert: GCIA
- 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 11.

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.

Who Should Attend

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

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 VMware 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

"Mike Poor is an excellent instructor. He has real world examples of the things he is teaching. He is able to infuse some fun in a rather dry subject. Bit Masking is not exactly scintillating, but he did a good job with it and he kept my interest."
-Karla Volpi, Tohono O'odham Community College

"SEC503 is a great course for both experienced and intermediate skill levels. I very much enjoy the hands on exercises."
-Kyler McClelland, USN

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.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Dave Shackleford

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

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

"SEC504 teaches not just how to do Incident Response, but most importantly, what not to do."
-Brad Milhorn, ii2P LLC

"SEC504 provides practice to the theory, and the knowledge I've gained is very valuable. Demonstrating, a buffer overflow, trumps just saying the term. Keep up the great work!"
-Mike Boya, Warner Bros.

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book "Virtualization Security: Protecting Virtualized Environments," as well as the coauthor of "Hands-On Information Security" from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Kevin Johnson

- GIAC Cert: GWAPT
- Cyber Guardian
- Masters Program

"The techniques I was taught in SEC542 proved so effective to my organization, my organization sent me to SEC642 six months later!"
-Karl Larson, NAVSUP

"Absolutely essential if you plan to pen test."
-Darrell Marsh, Attorney's Title Fund Services, LLC

"This course is the best way to hit the ground running in web app pen testing. I am excited to put all of my new skills to work!"
-Michael Dobb, CorelP Solutions

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

GWAPT
www.giac.org

SANS INSTITUTE
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

Kevin Johnson *SANS Senior Instructor*

Kevin Johnson is a Senior Security Consultant with Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture, and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises, and penetration testing everything from government agencies to Fortune 100 companies. Kevin is an instructor and author for the SANS Institute and a contributing blogger at TheMobilityHub. Kevin has performed a large number of trainings, briefings, and presentations for both public events and internal trainings. Kevin teaches for the SANS Institute on a number of subjects. He is the author of three classes: SEC542, SEC642, and SEC571. Kevin has presented at a large number of conventions, meetings, and industry events. Some examples of these are: DerbyCon, ShmooCon, DEFCON, Blackhat, ISACA, Infragard, and ISSA. In addition, Kevin is very involved in the open source community and runs a number of open source projects. These include SamuraiWTF, a web pen-testing environment; Laudanum, a collection of injectable web payloads; Yokoso!, an infrastructure fingerprinting project; and a number of others. Kevin is also involved in MobiSec and SH5ARK. Kevin was the founder and lead of the BASE project for Snort before transitioning that to another developer.

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
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

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.

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

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.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian

"Incredible course and very well laid out. Excellent tool kit DVD to use after class and very well taught. One of the BEST SANS classes I've taken yet. Ed's an excellent instructor and is a 'good man'!"
- Jeffrey Blasnitz, FBI

"After only one day, I already feel I have a more structured approach and understanding of pen testing. Having instructors like Skoudis who are working in the real world, successfully, and also writing the course is critical to the quality of SANS courses."
-Lawrence Wolfenden, FBI

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.

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Joshua Wright

- GIAC Cert: GMOB
- Masters Program

SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 11.

"SEC575 material is very good. Continuing to associate material with potential impact to organizations is key."
-Eugene Melendez, PwC

"SEC575 provided a good foundation for some of the key security issues and risks with using mobile devices at a managerial level, and also included some hands on analysis."
-Ben Duff, QA

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.

Who Should Attend

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

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.

GMOB
www.giac.org

SANS INSTITUTE
www.sans.edu

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions cyber warriors in the US military, government agencies, and critical infrastructure providers.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
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

"Excellent course, invaluable hands-on experience taught by people who not only know the tools and techniques, but know their quirkiness through practical, real-world experience."
-John Alexander, US Army

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: Advanced Computer Forensic Analysis and Incident Response 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

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. Rob frequently contributes articles at the SANS Blog http://computer-forensics.sans.org.

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Hal Pomeranz
- GIAC Cert: GREM
- Masters Program

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

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!

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

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. The course 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.

"FOR610 course is valuable because it helped me to see the tools being used to compromise systems, understand what is being infiltrated, and design ways to hinder that."
-Darian Lewis,
Fidelis Security Systems

"FOR610 has deepened my malware understanding; it encompasses a solid process for malware analysis."
-Charles Zammit, USAF

www.giac.org

www.sans.edu

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is the founder and technical lead for Deer Run Associates, a consulting company focusing on Digital Forensics and Information Security. He is a SANS Faculty Fellow and the creator of the SANS/GIAC Linux/Unix Security Track (GCUX), as well as being an instructor in the SANS Forensics curriculum. An expert in the analysis of Linux and Unix systems, Hal provides forensic analysis services through his own consulting firm and by special arrangement with MANDIANT. He has consulted on several major cases for both law enforcement and commercial clients. Hal is a regular contributor to the SANS Computer Forensics blog (http://computer-forensics.sans.org/blog) and co-author of the weekly Command-Line Kung Fu blog (http://blog.commandlinekungfu.com).

AUDIT 507

Auditing Networks, Perimeters, and Systems

SANS

Six-Day Program
Mon, Jan 20 - Sat, Jan 25
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: James Tarala

- GIAC Cert: GSNA
- Masters Program
- DoDD 8570

SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. More info on page 11.

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.

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

"In 18 years of auditing, this course offered the best mix of theoretical and technical by far, compared to any other training I have attended."
-John Poole,
Astec Industries, Inc.

"I really enjoyed learning a practical risk assessment approach with tools to enable me to determine root cause and consequences."
-Willy Alvarado, Protiviti

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.

www.giac.org

www.sans.edu

www.sans.org/8570

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.

SANS Simulcast

You don't have to miss out on SANS' top-rated training. Attend select Security East 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.

The following courses will be available via SANS Simulcast:

SEC401 | SEC503 | SEC575 | AUD507

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

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - 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.
  - 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.

SANS SECURING THE HUMAN

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

SECURITY EAST 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.

Keynote: Defending Networks in Uncertain Times *Dr. Eric Cole*

Attacks are always changing and in many cases an adversary can bypass an organization's defensive measures. Frequently, significant money is spent on cyber security with minimal positive return. This leads to frustration across the entire organization. Defensible measures need to be developed that can be tracked against metrics and implemented across an organization. If organizations focus on proper security measures, effective security can be implemented. Do not give up hope because in this talk, organizations will be given actionable things they can do to protect a network.

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. Not only can administrators completely administer and audit 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 will introduce students to using PowerShell scripts for assessing the security of these Microsoft services.

10 Things Security Teams Need to Know About Cloud Security *Dave Shackleford*

In this presentation, Dave will discuss ten key points that all security teams should understand about cloud infrastructure and security. Attendees will walk away with: 1) Ten concrete areas of cloud security focus, with takeaways from each; 2) Ideas for how to improve cloud security assessment and audit programs; 3) Technologies that should be evaluated now and in the near future for solving cloud security challenges; 4) Examples of what other organizations are doing to address these challenges.

Who's Watching the Watchers? *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation and aggregation... but do we know if we have it right? Will we detect the NextGen™ attackers? In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

Hacking Your Friends and Neighbors For Fun *Joshua Wright*

I regularly see my neighbors trying to connect to open wireless APs I run in my house. A while back, I set up a special open AP to give them Internet access. The cost? My entertainment. My neighbor-hack AP is set up to manipulate the web traffic of its users, randomly redirecting people to websites of my choosing, manipulating the format and content of pictures they download and more. In this talk, I'll show you how to set up your own neighbor-hack AP and, in the process, you'll learn just how scary (or fun) an open wireless AP can be.

Legends: The Reality Behind the Security Fairytales We All Hear! *Kevin Johnson*

In this talk, Kevin Johnson of Secure Ideas will walk through many of the behaviors and processes that security awareness classes talk about. We will explore the "what" of security practices that many people hear about but don't understand. And then we will walk through examples of behaviors that weaken security along with the real-world attacks that abuse these mistakes everyone makes.

Have no fear - DFIR is here! *Rob Lee, Hal Pomeranz*

In an age of darkness, at a time of evil...When the cyberworld needed heros, what it got was this team. In less time than it takes you to watch the Avengers, the DFIR hero team will take you through an end-to-end investigation starting with core steps in digital forensics, incident response, memory analysis, and RE Malware. Rob Lee and Hal Pomeranz will step through how key skills are used to solve a single case for 20 minutes each. The tag team approach will detail how teams can be leveraged in your environment to effectively respond to incidents on a single system and the enterprise. Two forensicators, 1 million hackers- the odds are just about even.

Vendor Showcase

Wed, January 22 | 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.

How Are You Protecting Your

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 20 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

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

Get Certified at **www.giac.org**

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 DoD 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

FUTURE SANS TRAINING EVENTS

SANS Pen Test Hackfest
TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

www.sans.org/event/pen-test-hack-fest-2013

SANS San Diego 2013

San Diego, CA | November 18-23

www.sans.org/event/san-diego-2013

SANS San Antonio 2013

San Antonio, TX | December 3-8

www.sans.org/event/san-antonio-2013

SANS Cyber Defense Initiative 2013

Washington, DC | December 12-19

www.sans.org/event/cyber-defense-initiative-2013

SANS Golden Gate 2013

San Francisco, CA | December 16-21

www.sans.org/event/sans-golden-gate-2013

SANS AppSec 2014

Austin, TX | February 3-8

www.sans.org/event/appsec-2014

SANS Scottsdale 2014

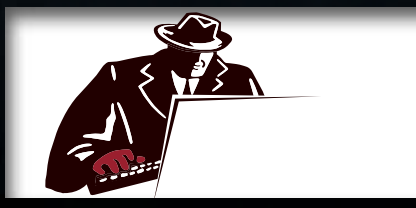
Scottsdale, AZ | February 17-22

www.sans.org/event/scottsdale-2014

SANS Cyber Guardian 2014

Baltimore, MD | March 3-8

www.sans.org/event/cyber-guardian-2014



SANS DFIRCON 2014

Monterey, CA | March 5-10

www.sans.org/event/dfircon-monterey-2014

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events
Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers
www.sans.org/security-training/by-location/all

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

OnSite
Live Training at Your Office Location
www.sans.org/onsite

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

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

ONLINE TRAINING

OnDemand
E-learning available anytime, anywhere, at your own pace
www.sans.org/ondemand

vLive
Convenient online instruction from SANS' top instructors
www.sans.org/vlive

Simulcast
Attend a SANS training event without leaving home
www.sans.org/simulcast

CyberCon
Live online training event
www.sans.org/cybercon

SelfStudy
Self-paced online training for the motivated and disciplined infosec student www.sans.org/selfstudy

SANS SECURITY EAST 2014

Hotel Information

Training Campus
Sheraton New Orleans

500 Canal Street
New Orleans, LA 70130
www.sans.org/event/security-east-2014/location

Special Hotel Rates Available

A special discounted rate of $189.00 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 December 27, 2013. To make reservations please call (888) 627-7033 and ask for the SANS group rate.

The Sheraton New Orleans Hotel is located in the heart of the Big Easy, right in the middle of an atmosphere of endless excitement from one of the world's greatest cities. Awake to a breakfast of beignets and cafe au lait just steps from the French Quarter. Relax in Jackson Square or dine at a world famous restaurant in the French Quarter. Hear the sultry tones of a late night jazz show. Place yourself in the middle of all the things to do in New Orleans!

Top 5 reasons to stay at the Sheraton New Orleans

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 Sheraton New Orleans, 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 Sheraton New Orleans that you won't want to miss!
5. Everything is in one convenient location!

SANS SECURITY EAST 2014

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/security-east-2014

To register, go to www.sans.org/event/security-east-2014

Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course:

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.

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at **301-654-7267** 9am - 8pm ET.

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 **December 25, 2013** – processing fees may apply.

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

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	11/27/13	$400.00	12/11/13	$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.*

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**