THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Baltimore 2014

Baltimore, MD September 22-27

Choose from these popular courses:

Advanced Exploit Development for Penetration Testers ***NEW!***

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Windows Forensic Analysis

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

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

Auditing Networks, Perimeters, and Systems

Advanced Security Essentials – Enterprise Defender

Perimeter Protection In-Depth

"SANS is awesome, and presents excellent and relevant information."

-Matthew Britton, BCBSLA

GIAC Approved Training

Register at sans.org/event/baltimore-2014

Save $400

by registering early!

See page 17 for more details.

We are pleased to invite you to the **SANS Baltimore 2014** training event from **September 22-27, 2014**. The event offers nine six-day courses, and the tuition includes special **SANS@Night** evening presentations to enhance your training.

The team of SANS instructors for this event includes many of the most knowledgeable experts in the security industry: Dr. Eric Cole, David Hoelzer, Paul A. Henry, Stephen Sims, Seth Misenar, Kevin Fiscus, Keith Palmgren, Alissa Torres, Jess Garcia, and Clay Risenhoover. The team will ensure that you not only learn the material, but that you will be able to use what you have mastered the day you get back to your office.

SANS Baltimore 2014 features hands-on immersion courses chosen to prepare you for a cybersecurity position or to enhance your career in this fast-growing field. Courses cover such topics as IT security, forensics, IT audit, and security management, and most are associated with one of 27 GIAC certifications that correspond to your specific skills. Five of the certifications will prepare you or your technical staff for DoD Directive 8570. Please use this brochure to view our comprehensive course descriptions, instructor bios, and evening event talks.

The brochure also provides information about earning a master's degree in Information Security Management (MSISM) or Engineering (MSISE) through the **SANS Technology Institute**, which is the only accredited graduate institution focused solely on cybersecurity.

SANS Baltimore 2014 takes place at the ***Sheraton Inner Harbor***, just steps away from the city's Inner Harbor and Oriole Park at Camden Yards. Baltimore's Inner Harbor is an attraction in itself: the National Aquarium features more than 16,000 marine animals, and the displays at the Maryland Science Center include two-story dinosaurs. Visit www.baltimoretourism.com for a complete list of attractions.

A special discounted rate of $189 S/D will be honored at the Sheraton Inner Harbor 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 August 29, 2014.

Now more than ever, top-quality, hands-on information security training will set you apart from others in the field. ***Register today for SANS Baltimore 2014*** and get the best computer security training money can buy!

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

"This is my third SANS class and the instructors are always excellent."
-Todd Grant, Sallie Mae

"It's a good sign if you come into the course concerned about the material and leave confident at the end of the lesson."
-David Fawley, ANSYS, Inc.

"SANS has the best subject matter experts in the world giving their training courses."
-Chip Snowden, Global Payments

SC MAGAZINE AWARDS 2014 WINNER
Honored in the U.S.

Courses-at-a-Glance

@SANSInstitute *Join the conversation:* #SANSBaltimore

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Seth Misenar

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

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

"SEC401 lays a security foundation to build a good understanding of how to approach security in an enterprise."
-Derek Lewis, State of CT

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.

"I love how a concept that confuses so many people is made easy to understand through the brilliant use of simple analogies. This fast-paced high-volume course is filling in gaps, and flushing other things out, all with very memorable examples."
-Michael Decker, CNS Security

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Seth Misenar *SANS Principal Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and 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. @sethmisenar

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Keith Palmgren

- GIAC Cert: GCED
- Masters Program
- DoDD 8570

SANS
sans.org

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 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

Cybersecurity continues to be a critical area for organizations and will 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.

"Love the content, course, and instructor. SEC501 will greatly enhance my effectiveness upon return to the office."
-Andrew D'Albor, CB&I

"SEC501 gives a hands-on technical overview and hands-on approach for admins – but also value added to non-admin personnel (analysts)."
-Stephen Pastore, General Electric

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.

giac.org

sans.edu

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.

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. @kplamgren

SECURITY 502

Perimeter Protection In-Depth

SANS

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Paul A. Henry

- GIAC Cert: GPPA
- Masters Program
- Cyber Guardian

There is no single fix for securing your network. That's why this course is a comprehensive analysis of a wide breadth of technologies. In fact, this is probably the most diverse course in the SANS catalog, as mastery of multiple security techniques is required to defend your network from remote attacks. You cannot just focus on a single OS or security appliance. A proper security posture must be comprised of multiple layers. This course was developed to give you the knowledge and tools necessary at every layer to ensure your network is secure.

The course material has been developed using the following guiding principles:

- **Learn the process, not one specific product.**
- **You learn more by doing, so hands-on problem solving is key.**
- **Always peel back the layers and identify the root cause.**

Who Should Attend

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network and system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

While technical knowledge is important, what really matters are the skills to properly leverage it. This is why the course is heavily focused on problem solving and root cause analysis. While these are usually considered soft skills, they are vital to being effective in the role of security architect. So along with the technical training, you'll learn risk-management capabilities and even a bit of Zen empowerment.

The course starts by looking at common problems we need to resolve. To secure your network you really need to understand the idiosyncrasies of the protocol. We'll talk about how IP works and how to spot the abnormal patterns. Then we'll learn how to control it on the wire. We focus on the underlying technology used by both good and bad products. By gaining knowledge of what goes on under the cover, you will be empowered to make good product choices for years to come.

Just because two firewalls are stateful inspection, do they really work the same on the wire? Is there really any difference between stateful inspection and network-based intrusion prevention, or is it just marketing? These are the types of questions we address in the next portion of the course.

giac.org

From there, it's a hands-on tour through how to perform a proper wire-level assessment of a potential product, as well as what options and features are available. We'll learn how to deploy traffic control while avoiding some of the most common mistakes.

sans.edu

A properly layered defense needs to include each individual host – not just the hosts exposed to access from the Internet, but hosts that have any kind of direct or indirect Internet communication capability as well. We'll start with OS lockdown techniques and move on to third-party tools that can permit you to do anything from sandbox insecure applications to full-blown application policy enforcement.

sans.org/
cyber-guardian

"SEC502 covers a lot of very relevant information to security as a whole."
-Scott Lussier, Draper Laboratory

"Paul did an excellent job throughout the week of covering complex material in a very simple manner."
-Maurice Garcia, UPS

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. @phenrycissp

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS
sans.org

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Kevin Fiscus

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

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

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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

"Fantastic learning experience. So much information presented in an understandable manner."
-Scotlyn Monk, Ingalls Information Security

"The labs were great, they were real-world activities that I will be able to use going forward."
-Larry Petty, Tribridge

Kevin Fiscus *SANS Certified Instructor*

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

SECURITY 760

Advanced Exploit Development for Penetration Testers

NEW

SANS
sans.org

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Stephen Sims

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 one-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

SANS Brochure Challenge

-... .. - ... - --- .--. .-.. -.-- ... .-.. .- ... .---- .--- --.. .-.. -.. ----- -.

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

"SEC760 is the kind of training we couldn't get anywhere else. It's not all theory, we were able to implement and exploit everything we learned."
-Jenny Kitaichit, Intel

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant. He has spent many years performing security architecture, exploit development, reverse engineering, and penetration testing. Stephen has an MS in information assurance from Norwich University. He is the author of SANS' only 700-level course, SEC710: Advanced Exploit Development, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on *SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking*. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. @Steph3nSims

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Alissa Torres
- GIAC Cert: GCFE
- Masters Program

Master Windows Forensics – What Do You Want to Uncover Today?

Every organization will deal with cyber crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

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

Digital Forensics and Incident Response
digital-forensics.sans.org

FOR408: Windows Forensic Analysis focuses on the critical digital forensics knowledge of the Microsoft Windows operating system. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 7 artifacts.

This course utilizes a brand-new Windows 8.1 based case exercise that took over 6 months to create the data. Realistic example case data takes months to create in real time correctly. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. Our development team spent months creating an incredibly realistic scenario. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The brand new case workbook, will detail the step-by-step each investigator could follow to examine the latest technologies including Windows 8.1.

"Awesome coverage. FOR408 covers material in logical fashion going from 0-60 in windows forensics."
-Reed Puchron, EY

"FOR408 is a great course to get into content activities and forensics, and covers a large number of tools which is great."
-Brett Eckert, Weatherford

giac.org

sans.edu

Alissa Torres *SANS Certified Instructor*

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

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS sans.org

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jess Garcia
- 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 instructor was knowledgeable, engaging, and extremely helpful."
-Ron Brown, USAA

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.

giac.org

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.edu

Jess Garcia *SANS Principal Instructor*

Jess Garcia, founder of One eSecurity, is a Senior Security Engineer with over 15 years of experience in Information Security. During the last 5 years Jess has worked in highly sensitive projects in Europe, USA, Latin America and the Middle East with top global customers in sectors such as financial & insurance, corporate, media, health, communications, law firms or government, in areas such as Incident Response & Computer Forensics, Malware Analysis, Security Architecture Design and Review, etc. Previously, Jess worked for 10 years as a systems, network and security engineer in the Spanish Space Agency, where he collaborated as a security advisor with the European Space Agency, NASA, and other international organizations. Jess is a frequent speaker at security events, having been invited to dozens of them around the world during the last few years. Jess has also contributed to several books, articles, SANS courseware, the GIAC program, etc. Jess is an active security researcher in areas such as Incident Response and Computer Forensics or Honeynets. He is currently a SANS Principal Instructor. Jess holds a Masters of Science in Telecommunications Engineering from the Univ. Politecnica de Madrid. @j3ssgarcia

MANAGEMENT 414

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

SANS sans.org

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
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: Dr. Eric Cole

- GIAC Cert: GISP
- DoDD 8570

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

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

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

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.

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

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.

giac.org

sans.org/8570

"Eric did an amazing job teaching this course MGT414. It was a lot of material, but he did a good job of keeping the class going. Thanks, I'll be back for future classes."
-Axel Persaud,
University of Maryland

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. @drericcole

AUDIT 507

Auditing Networks, Perimeters, and Systems

SANS
sans.org

Six-Day Program
Mon, Sept 22 - Sat, Sept 27
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructors:
David Hoelzer &
Clay Risenhoover

- GIAC Cert: GSNA
- Masters Program
- DoDD 8570

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 helping management 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

giac.org

sans.edu

sans.org/8570

SANS Instructor
Clay Risenhoover

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clays past experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sector. He has a masters degree in computer science and holds a number of technical and security certifications, including GPEN, GSNA, CISA, CISM, and CISSP.

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is the author of more than 20 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 25 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. @david_hoelzer

BALTIMORE 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: APT: It is Time to Act *Dr. Eric Cole*

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

Extracting User Credentials using Memory Forensics *Alissa Torres*

Though Windows credential extraction and password cracking are often categorized as offensive skills, used by pentesters and sophisticated attackers, digital forensic examiners and incident responders can also put these techniques to use to further their investigations. Just by parsing a physical memory image of a Windows system, local and domain user account password hashes can be pulled from the registry hives and plaintext credentials can be extracted from the wdigest in the lsass process for logged-on users. For employee or criminal investigations, cracking a user's logon password can allow the examiner access to encrypted files or accounts due to frequent password re-use by users. Likewise, in intrusion cases, being able to dump credentials from a compromised system allows the IR team to assess what accesses the attacker was able to acquire, providing for better scoping of the intrusion. This webcast walks through several practical forensics use cases for Windows credential extraction from memory and includes excerpts from the ***SANS FOR526: Memory Forensics In-Depth*** class.

From APT to AVT – Investigating the Latest Threats *Jess Garcia*

APT (Advanced Persistent Threat) attacks can no longer be considered new. However, the techniques behind those attacks continue evolving, and now drive-by and watering hole attacks are slowly replacing the traditional spear-phising. At the same time the Dark Side continues evolving towards more effective attacks that can bypass our defenses. AVT (Advanced Volatile Threat) seems to be getting more and more popular, as well as sophisticated Zero-Day Malware, Ransomware, POS Malware, Android Malware or even Airgap Jumping Malware. Protecting our organizations against these threats is getting more and more difficult, and a new trend towards early detection and rapid response seems to be emerging in the defensive community. In this talk Jess Garcia will be dissecting this new breed of attacks, and will show how a combination of different forensic techniques can be effective in the detection, investigation, and analysis of such attacks.

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.

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

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

Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password". The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

Continuous Ownage: Why you Need Continuous Monitoring

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 Conrad's new course: ***SEC511: Continuous Monitoring and Security Operations***.

Vendor Showcase

Wednesday, September 24 | 10:30-10:50am | 12:00-1:30pm | 3:00-3:20pm

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.

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.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III
A+CE Network+CE SSCP	**GSEC** Security+CE SSCP	**GCED** **GCIH** **CISSP** (or Associate) CISA

IAM Level I	IAM Level II	IAM Level III
GSLC CAP Security+CE	**GSLC** **CISSP** (or Associate) CAP, CASP CISM	**GSLC** **CISSP** (or Associate) CISM

Computer Network Defense (CND) Certifications

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

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

GCWN **GCUX**

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.

SANS TRAINING COURSE	DoDD APPROVED CERT
SEC401	GSEC
SEC501	GCED
SEC503	GCIA
SEC504	GCIH
AUD507	GSNA
FOR508	GCFA
MGT414	CISSP
MGT512	GSLC

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

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

MAKE YOUR NEXT MOVE COUNT

EARN A RESPECTED GRADUATE DEGREE

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

Master's Degree Programs:

- **M.S. IN INFORMATION SECURITY ENGINEERING**
- **M.S. IN INFORMATION SECURITY MANAGEMENT**

Specialized Graduate Certificates:

- **PENETRATION TESTING & ETHICAL HACKING**
- **INCIDENT RESPONSE**
- **CYBERSECURITY ENGINEERING (CORE)**

Top Reasons Students Choose SANS Graduate Programs:

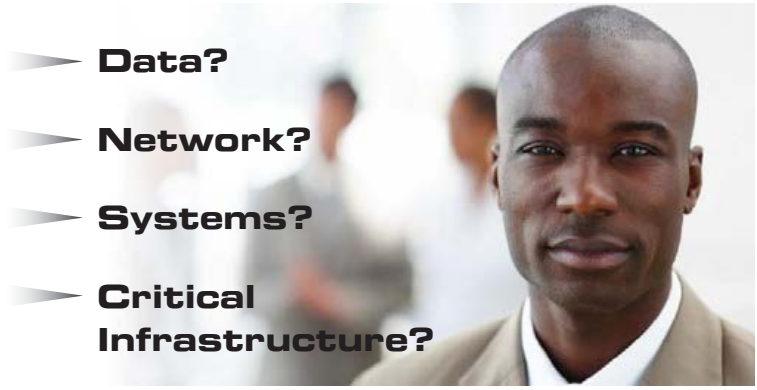
- World-class, cutting-edge technical courses that refine and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership and who bring the material to life
- Simulation and group projects that teach students to write, present, and persuade effectively
- Validation from multiple GIAC certifications even before you earn your degree
- 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 recognize and respect a master's degree from SANS

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

Learn more at
sans.edu
info@sans.edu

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

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 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

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

Global Information Assurance Certification GIAC www.giac.org

Get Certified at **giac.org**

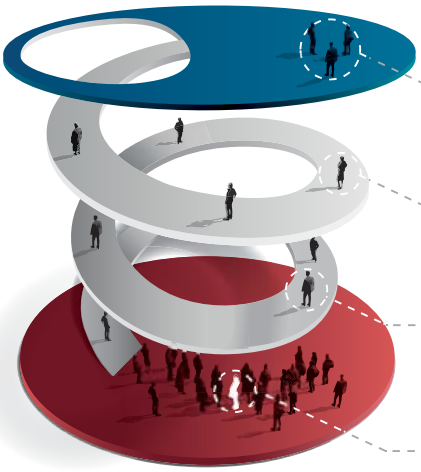
SANS CyberTalent Powered by GIAC

Contact Us to Learn More

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 TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

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 computer based training modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - 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

FUTURE SANS TRAINING EVENTS

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

SANS Boston 2014

Boston, MA | July 28 - August 2

SANS San Antonio 2014

San Antonio, TX | August 11-16

Cyber Defense
SUMMIT & TRAINING

Nashville, TN | August 13-20

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

SANS Chicago 2014

Chicago, IL | August 24-29

SANS Crystal City 2014

Crystal City, VA | September 8-13

Retail Cyber Security
SUMMIT & TRAINING

Dallas, TX | September 8-17

Security Awareness
SUMMIT & TRAINING

Dallas, TX | September 8-17

SANS Albuquerque 2014

Albuquerque, NM | September 15-20

SANS BALTIMORE 2014

Hotel Information

Training Campus
Sheraton Inner Harbor

300 South Charles Street
Baltimore, MD 21201
sans.org/event/baltimore-2014/location

The Sheraton Inner Harbor Hotel surrounds you with the best of Baltimore. Connected to The Baltimore Convention Center and steps from the magnificent Inner Harbor and Oriole Park at Camden Yards, we are convenient to everything that makes our city so wonderful.

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 August 29, 2014.

Top 5 reasons to stay at the Sheraton Inner Harbor

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 Inner Harbor, 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 Inner Harbor that you won't want to miss!
5. Everything is in one convenient location!

SANS BALTIMORE 2014

Registration Information

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

Register online at sans.org/event/baltimore-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	**8/6/14**	**$400.00**	**8/20/14**	**$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 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 September 3, 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.
sans.org/vouchers