THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

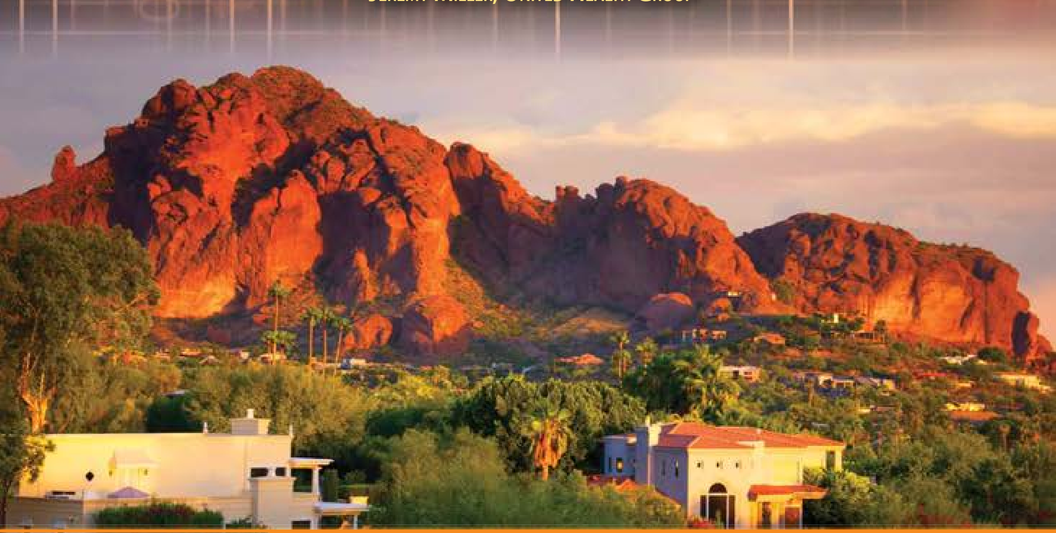
SANS

Scottsdale 2014

Scottsdale, AZ | February 17-22

SANS Exceptional Training comes to Scottsdale in February

"The methodical approach and real-world examples made this course interesting, informative, and applicable to my job."
-Jeremy Miller, United Health Group



Choose from these popular courses:

SEC401: **Security Essentials Bootcamp Style**

SEC560: **Network Penetration Testing and Ethical Hacking**

FOR508: **Advanced Computer Forensic Analysis and Incident Response**

SEC566: **Implementing and Auditing the Twenty Critical Security Controls – In-Depth**

SEC301: **Intro to Information Security**

SEC502: **Perimeter Protection In-Depth**

GIAC Approved Training

Register at www.sans.org/event/scottsdale-2014

Save $400 by registering early! See page 13 for more details.

SANS is returning to **Scottsdale** in 2014 from **February 17-22**. We are bringing our top courses in IT security, pen testing, and computer forensic analysis. Our instructor lineup scheduled for Scottsdale includes: Dr. Eric Cole, Fred Kerby, Paul A. Henry, Randy Marchany, Alissa Torres, and Adrien de Beaupre. These instructors not only have real-world experience, but ensure you will be able to apply our information security training the day you get back to the office!

Five of our six courses are associated with **GIAC Certification**, and two courses align with **DoD Directive 8570.** To learn more, visit our GIAC webpage at **www.giac.org** and register for your certification attempt today. SEC401 and SEC566 may also be taken to earn credit toward a master's degree at **SANS Technology Institute** (STI) once you have applied. See our STI webpage at **www.sans.edu** for more information and apply today!

Our SANS Scottsdale 2014 campus is the **Hilton Scottsdale Resort & Villas** in the heart of the city. This hotel has views of Camelback Mountain, and it is close to shopping, dining, attractions, and world-class golf. Within 25 miles are the Arizona State Capitol, Camelback Mountain, Chase Field, Desert Botanical Gardens, Heard Museum (American Indian arts/culture), Phoenix Art Museum, Phoenix Zoo, Pueblo Grande Museum, Taliesin West, and an 1880s-style western frontier town called Rawhide! And remember, Scottsdale's average high temperature in February is 73 degrees, so this might be a nice winter break.

A special discounted rate of $179.00 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 January 24, 2014. See our registration page for complete information.

Register by December 25 and save $400. Start making your training and travel plans now; let your colleagues and friends know about **SANS Scottsdale 2014**. We look forward to seeing you there.

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

"Security is a big focus for our IT organization. This face-to-face training, with the experiences of other companies, is a very effective way to learn."
-Michael Stothers,
The Boeing Company

"I had no idea of the legal side of incident handling. SEC401 material was really eye-opening."
-Renato Luiz Cunha,
EMBRAER

"SEC566 provided a very practical way of implementing real controls to system security."
-Peter Kiilu, Niche Forensic and Risk Management Consulting, LLC

"Cutting-edge expertise taught by world-class experts."
-Joseph Murray, Deloitte

Courses-at-a-Glance

<table>
<tr><th></th><th></th><th>MON 2/17</th><th>TUE 2/18</th><th>WED 2/19</th><th>THU 2/20</th><th>FRI 2/21</th><th>SAT 2/22</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security</td><td colspan="5">Page 1</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">Page 2</td></tr>
<tr><td>SEC502</td><td>Perimeter Protection In-Depth</td><td colspan="6">Page 3</td></tr>
<tr><td>SEC560</td><td>Network Penetration Testing and Ethical Hacking</td><td colspan="6">Page 4</td></tr>
<tr><td>SEC566</td><td>Implementing and Auditing the Twenty Critical Security Controls – In-Depth</td><td colspan="5">Page 5</td><td></td></tr>
<tr><td>FOR508</td><td>Advanced Computer Forensic Analysis and Incident Response</td><td colspan="6">Page 6</td></tr>
</table>

SECURITY 301

Intro to Information Security

Five-Day Program
Mon, Feb 17 - Fri, Feb 21
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Fred Kerby
▶ GIAC Cert: GISF

Course updated to include hands-on labs!

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

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

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

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

www.giac.org

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

"As an introduction course, SEC301 is a must for anyone in the information security field. I wish I had taken it two years ago."
-Joanne Woodsen, Vanguard

"SEC301 provided me with an excellent review and brought to my attention some necessary changes to our network security."
-Terry Benes, University of Nebraska Foundation

"It is hard not to be excited about security when the instructor is so excited about the topic. It makes me want to put all of my employees through SEC301."
-Ron Austin, Sony

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, Feb 17 - Sat, Feb 22
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

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.

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.

"SEC401 took what I thought I knew and truly explained everything to me. Now, I understand security essentials and know how and why we apply them. I loved the training and can't wait to come back for more."
-Nicholas Blanton, ManTech International

www.giac.org

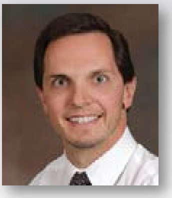
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

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 analyst, 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



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 502

Perimeter Protection In-Depth

Six-Day Program
Mon, Feb 17 - Sat, Feb 22
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.

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

Is there traffic passing by my firewall I didn't expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We'll dig into these questions and more and answer them.

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.

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.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

"The course is very valuable because it shows you the techniques and methods attackers use and how to defend against them."
-Curtis Greer, U.S. Navy

"SEC502 opened my eyes so wide it scared me!"
-George Scarborough, Defense Logistics Agency

"As an analyst, these courses are the most relevant in the industry."
-Louis Robichaud, Atlantic Lottery Corp.

Paul A. Henry *SANS Senior Instructor*

Paul Henry is 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. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the Information Security Management Handbook, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/scottsdale-2014/courses

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Feb 17 - Sat, Feb 22
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Adrien de Beaupre

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

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

"The Network Penetration and Ethical Hacking course provided me with good practice and tools for me to provide to my customers."
-Florent Batard, SCRT

"SEC560 helped me to take the stew of ideas and techniques in my head and organize them in a professional and usable way."
-Richard Tafoya,
Redflex Traffic Systems

"SEC560 presents great content, real-world expertise and application."
-Brice Toth, PSU

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

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

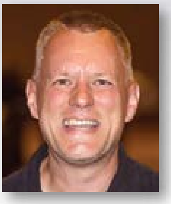
We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then, we discuss a time-tested methodology for penetration and ethical hacking across the network,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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian



Adrien de Beaupre *SANS Instructor*

Adrien de Beaupre is a senior Information Security Consultant with Intru-Shun.ca Inc., experienced in penetration testing and incident response. Mr. de Beaupre holds the ISC2 CISSP, GXPN (GIAC Exploit Researcher and Advanced Penetration Tester), GWAPT (GIAC Web Application Penetration Tester), GPEN (GIAC Penetration Tester), GCIH (GIAC Certified Incident Handler), GSEC (GIAC Security Essentials), OPST (OSSTMM Professional Security Tester), and OPSA (OSSTMM Professional Security Analyst) certifications. As a volunteer member of the SANS Internet Storm Center (isc.sans.edu) he performs incident handling and threat analysis duties. When not geeking out he can be found with his family, or at the dojo.

SECURITY 566

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

Five-Day Program
Mon, Feb 17 - Fri, Feb 21
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Randy Marchany

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

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

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

The British governments Center for the Protection of National Infrastructure describes the Controls as the baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.

SANS in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC440, SEC401, SEC501, MGT512, and other SANS Audit courses

"I perform risk assessments regularly – SEC566 reinforces our methodology and provides new and updated information."
-Stacey Oliea, Emerson Electric

"Implementing the critical controls should be on everyone's roadmap. SEC566 gives great directions for making that journey!"
-Randy Pauli, Chelan County PUD

"SEC566 is an excellent resource for understanding IT infrastructure, and what tools to use and when to use them."
-Rick Ramsingh, Knowledge Consulting Group, Inc.

Randy Marchany *SANS Certified Instructor*

Randy is the Chief Information Security Officer of Virginia Tech and the Director of Virginia Tech's IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. He is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks of 2000.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program
Mon, Feb 17 - Sat, Feb 22
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Alissa Torres

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

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

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.

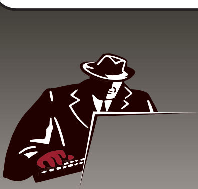
During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/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

"Best forensics training I've had so far. I thought the DCS courses were great but SEC508 is a lot more current and applicable to the real world! Excellent course and instructor overall!"
-Marc Bleicher, Bit9

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 a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

SCOTTSDALE 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.

OSSAMS: Putting the Sexy Back into Penetration Testing Analysis

Adrien de Beaupre

This presentation will discuss information security penetration testing methodology, and how portions of the test process may be automated. The analysis of test results can be made more efficient through development of additional tools to assist the analyst. I will present the Open Source Security Assessment Management System (OSSAMS) which is a framework for the automation, data collection, analysis, and reporting in penetration testing and vulnerability assessment efforts. OSSAMS is written in Python and allows for the processing of tool results, parsing and normalizing the data, extraction of meaningful information via query, and more effective analysis.

Offensive Digital Forensics *Alissa Torres*

Network intruders are utilizing increasingly more sophisticated offensive forensic techniques in order to parse remote systems, obtain credentials, and locate and steal "target data," all while flying under the radar of modern detection systems. Incident responders and forensic examiners must be able to unravel the actions and intent of the adversary on their own networks in order to halt their progress and anticipate future campaigns. From this session, attendees will gain a deeper understanding of today's offensive forensic strategies, how adversaries determine where key sensitive data and target individuals reside, and, most importantly, how to detect these techniques utilizing Windows and file system artifacts.

Cloud IR and Forensics *Paul A. Henry*

The move to private and public cloud changes many things, including how we respond for IR and forensics. As an example: traditionally in a physical realm we relied upon imaging a server's hard drive as well as RAM to perform a thorough analysis. Today in the cloud, creating a forensically sound image of an "instance" of a server to capture the server's abstracted hard disk and an image of its RAM brings new technical and legal complications. An additional issue to consider is that some vendor's platforms are simply not fully supported by our current IR & forensics tools; today's commercial tools lack the ability to perform any analysis at all on a VMware VMFS file system. Lastly, downloading a large server image may simply be cost prohibitive due to the high bandwidth costs associated with moving data out of the cloud environment. The best course of action may be to perform your analysis within the cloud - however, the methods used in the analysis within the cloud must be forensically sound and as always in computer forensics, they must be repeatable and the result must be the same findings. In this session we will begin to explore the changes that simply must be made to your IR and forensics procedures to properly address IR & forensics in the cloud.

GIAC Program Overview

SANS Technology Institute Open House

Vendor Showcase

Tuesday, February 18 | 10:30am-10:50am | 12:30pm-1:15pm | 3:00pm-3:20pm

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

The information security field is growing and maturing rapidly. Are you positioned to grow with it? A Master's Degree in Information Security from the SANS Technology Institute (STI) will help you build knowledge and skills in management or technical engineering.

The SANS Technology Institute (STI) offers two unique master's degree programs:

MASTER OF SCIENCE IN INFORMATION SECURITY ENGINEERING

MASTER OF SCIENCE IN INFORMATION SECURITY MANAGEMENT

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

Apply today!
Cohorts are forming now.
www.sans.edu

www.sans.edu

info@sans.edu

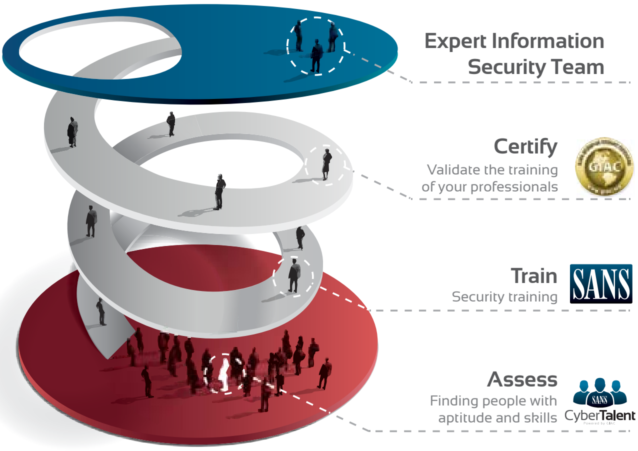
855-672-6733

SANS CyberTalent
Powered by GIAC

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

A Web-Based Recruitment and Talent Management Tool

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



Expert Information Security Team

Certify
Validate the training of your professionals

Train
Security training

Assess
Finding people with aptitude and skills

Benefits of SANS CyberTalent Assessments

For Recruiting

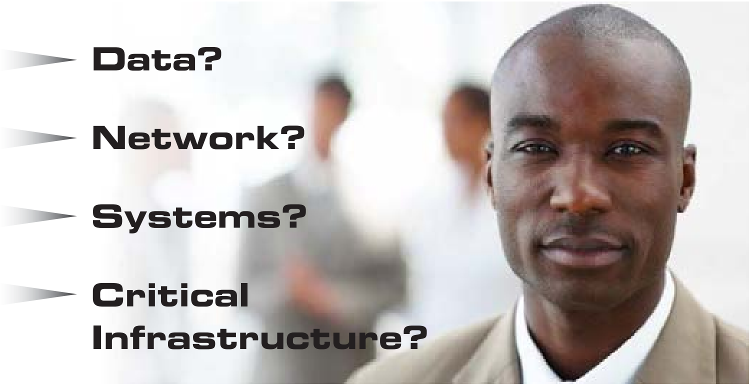
- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

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

How Are You Protecting Your



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

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

GIAC offers over 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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

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

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

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

SANS CYBER GUARDIAN PROGRAM

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

Real Threats

Real Skills

Real Success

Prerequisites

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

Core Courses

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

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

Blue Team Courses

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

Red Team Courses

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

Join Today!

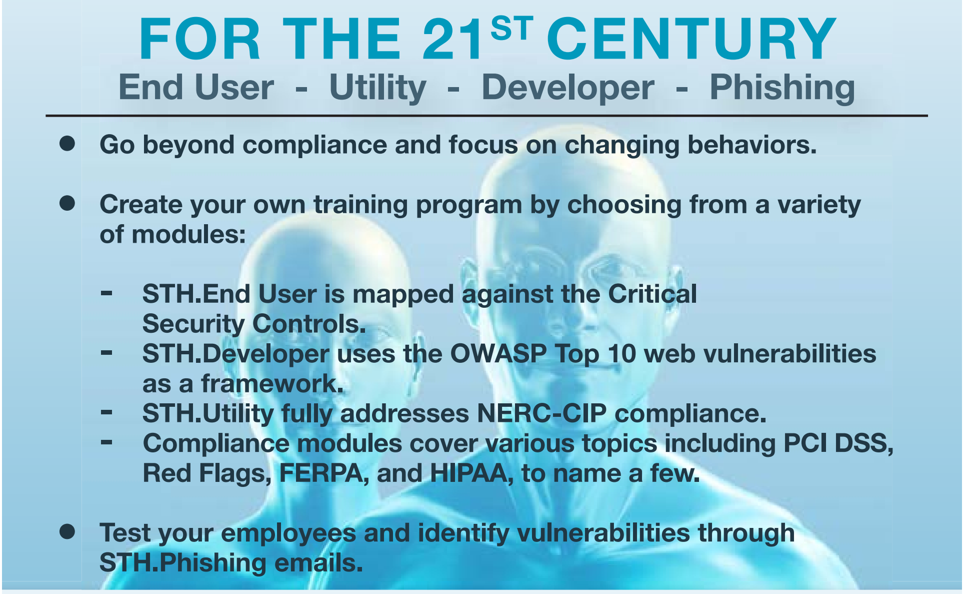
Contact us at
onsite@sans.org
to get started!

www.sans.org/cyber-guardian

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

FUTURE SANS TRAINING EVENTS

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 Security East 2014

New Orleans, LA | January 20-25

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

SANS AppSec 2014

Austin, TX | February 3-8

www.sans.org/event/appsec-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

ICS Security Summit 2014 - Orlando

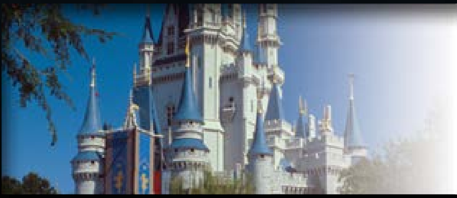
Lake Buena Vista, FL | March 12-18

www.sans.org/event/north-american-ics-scada-summit-2014

SANS Northern Virginia 2014

Reston, VA | March 17-22

www.sans.org/event/northern-virginia-2014



SANS 2014

Orlando, FL | April 5-14

www.sans.org/event/sans-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 SCOTTSDALE 2014

Hotel Information

Training Campus
Hilton Scottsdale Resort and Villas

6333 North Scottsdale Road
Scottsdale, AZ 85250
www.sans.org/event/scottsdale-2014/location

Special Hotel Rates Available

A special discounted rate of $179.00 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 January 24, 2014. To make reservations please call 800-445-8667 and ask for the SANS group rate.

The Hilton Scottsdale Resort & Villas is located in the heart of Scottsdale, within minutes of shopping, attractions, dining, and business districts. With breathtaking views of Camelback Mountain, this AAA Four Diamond resort combines a relaxed ambience with decor inspired by the Sonoran Desert. Relax in your beautifully furnished, spacious guest room. Upgrade to one of our villas and enjoy beautiful views from your private balcony, or swim in the private pool dedicated solely to the villas. The Hilton Scottsdale Resort & Villas promises an unforgettable stay.

Top 5 reasons to stay at the Hilton Scottsdale Resort & Villas

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

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

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

4 SANS schedules morning and evening events at the Hilton Scottsdale Resort and Villas that you won't want to miss!

5 Everything is in one convenient location!

SANS SCOTTSDALE 2014

Registration Information

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

To register, go to www.sans.org/event/scottsdale-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 **January 29, 2014** – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**12/25/13**	**$400.00**	**1/8/14**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5 - 9 people from the same organization register at the same time

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

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

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