THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Security East 2015

New Orleans, LA | January 16-21

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Windows Forensic Analysis

Web App Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

SANS Security Leadership Essentials For Managers with Knowledge Compression™

And more!

"This course is highly useful for giving me a sound baseline of technical and general skills to help me manage an effective team."

-Richard Ward, REA Group

GIAC Approved Training

Register at sans.org/event/security-east-2015

SAVE $400

by registering early!

See page 21 for more details.

Dear Colleague,

SANS is excited to return to the "Big Easy" for **SANS Security East 2015** on **January 16-21**. This year's event offers eleven courses, taught by SANS top-rated instructors, plus all courses are associated with *GIAC* certification. Keeping ahead of the persistent security threats requires not only diligence but cutting-edge training. Now is the time to improve your skills in information security, security management, and security forensics.

All of the courses at Security East 2015 will earn you credits that may be applied toward a *SANS Technology Institute* graduate program, including a *Master of Science in Information Security Engineering* or *Management* degree, or one of our graduate certificates (*Penetration Testing* or *Incident Response*). To learn more about SANS Cyber Degree Programs, go to sans.edu.

SANS Security East features bonus evening presentations including a keynote speaker sharing the latest threats as well as *Vendor* events where we'll discuss the best solutions. The full list of courses offered in New Orleans can easily be found on the *Courses-at-a-Glance* page with complete course descriptions and instructor bios on the pages that follow.

Put the skills you'll learn to practical use and join more than 60,000 GIAC certified professionals who make the cybersecurity industry safe! Visit our *GIAC* page (giac.org) for more information and register for your certification attempt today.

Our SANS Security East 2015 campus is at the **Hilton New Orleans Riverside**, in the heart of the Big Easy. The riverfront hotel is steps from the famous New Orleans Streetcar lines, a few blocks away from the French Quarter, and on the banks of the Mississippi River. While visiting New Orleans, see a plantation, shop at Riverwalk Marketplace or Canal Place, take a swamp tour, choose from over 45 museums, and eat unique food from some of the city's best restaurants. New Orleans is a fabulous destination with something of interest for everyone! A special discounted rate of $199 S/D will be honored based on space availability through December 22. Register today!

What makes SANS courses the best investment for information security training? You will be able to apply our information security training the day you get back to the office.

Join us in New Orleans for SANS Security East 2015 for the best security training your money can buy – we are looking forward to meeting you in New Orleans!

Ed Skoudis

Ed Skoudis
SANS Pen Testing Curriculum Lead

Ed Skoudis,
SANS Faculty Fellow

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

"I'm not sure what the next five days might be, but what I've learned this first day is worth the money I paid for the entire class."
-Tung Neuyen, Denver Water

"What a fabulous course and very relevant skills you can take back and use right away. Best training on the market!"
-Rob McBee, SMUD

"As a director of IT, this course showed me what my security team should be doing."
-Brian Bounds, Texas Biomedical Research Institute

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

COURSES-AT-A-GLANCE

		FRI 1/16	SAT 1/17	SUN 1/18	MON 1/19	TUE 1/20	WED 1/21
SEC401	Security Essentials Bootcamp Style	Page 2					
SEC501	Advanced Security Essentials – Enterprise Defender	Page 3					
SEC503	Intrusion Detection In-Depth	Page 4					
SEC504	Hacker Tools, Techniques, Exploits & Incident Handling	Page 5					
SEC542	Web App Penetration Testing and Ethical Hacking	Page 6					
SEC560	Network Penetration Testing and Ethical Hacking	Page 7					
SEC566	Implementing & Auditing the Critical Security Controls	Page 8					
SEC575	Mobile Device Security and Ethical Hacking	Page 9					
FOR408	Windows Forensic Analysis	Page 10					
FOR610	REM: Malware Analysis Tools and Techniques	Page 11					
MGT512	Security Leadership Essentials For Managers	Page 12					

Department of Defense Directive 8570

(DoDD 8570)

sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III	IAM Level I	IAM Level II	IAM Level III
A+CE Network+CE SSCP	**GSEC** (SEC401) Security+CE SSCP	**GCED** (SEC501) **GCIH** (SEC504) **CISSP** (MGT414) (or Associate) CISA	**GSLC** (MGT512) CAP Security+CE	**GSLC** (MGT512) **CISSP** (MGT414) (or Associate) CAP, CASP CISM	**GSLC** (MGT512) **CISSP** (MGT414) (or Associate) CISM

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA (SEC503) **GCIH** (SEC504) CEH	SSCP CEH	**GCIH** (SEC504) **GCFA** (FOR508) CSIH, CEH	**GSNA** (AUD507) CISA CEH	CISSP - ISSMP CISM

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I	IASAE II	IASAE III
CISSP (MGT414) (or Associate)	**CISSP** (MGT414) (or Associate) CASP	CISSP - ISSEP CISSP - ISSAP

Computer Environment (CE) Certifications

GCWN (SEC505) **GCUX** (SEC506)

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to giac.org to learn more about certification renewal.

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

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
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

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

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

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. Our course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- **What is the risk?**
- **Is it the highest priority risk?**
- **What is the most cost-effective way to reduce the risk?**

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

"This course gives me a much better understanding of the tools to use to help make networks more secure by pointing out vulnerabilities." -John McDonald, Florida Dept. of LE

giac.org

sans.edu

sans.org/cyber-guardian

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

"Eric is incredible; he never ceases to amaze me with his ability to relate the information to everyone while keeping the material interesting."
-Brian Ward, Jackson Supply

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

SECURITY 501

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor: Paul A. Henry

- GIAC Cert: GCED
- Masters Program
- DoDD 8570

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- Students 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

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

giac.org

sans.edu

sans.org/8570

"Dynamic, experienced, and puts everything in perspective! A must for cybersecurity professionals!"
-Gary Oakley, BMPC

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

"Paul is great and makes the class very interesting. I've been to many SANS classes but Paul's classes are by far the best."
-Fahad Alkhaldi, Saudi Aramco

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 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor

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

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Who Should Attend

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

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You'll get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

giac.org

sans.edu

sans.org/
cyber-guardian


sans.org/8570

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

"I find this training very valuable because it is comprehensive and the instructor is very knowledgeable."
-George Diolamou, Jacob's Engineering

"SANS training is the best in the world and with Mike teaching it makes it even better."
-Nicolas Stevens, CISCO

"Mike is great. He brings so much energy, passion, and knowledge to his class."
-Paul Madigan, INFOZEN

Mike Poor *SANS Senior Instructor*

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

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Bryce Galbraith

- 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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose 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. As defenders, it is essential we understand these hacking tools and techniques.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

"This course provides an understanding on how and what to do to handle an incident that I did not know."
-Palmer Taskerud, DOD

"The real-life examples talked about in class greatly reinforced what we were learning."
-Dan Gloughlin, Turbine, Inc

"I've enjoyed the labs and using the tools for each lab. It is great to actually see how the tools work."
-Christian Campbell, National Guard

Bryce Galbraith *SANS Principal Instructor*

As a contributing author to the international best-seller *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith

SECURITY 542

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor: Seth Misenar

- GIAC Cert: GWAPT
- Masters Program
- Cyber Guardian

Assess Your Web Apps in Depth

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

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

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

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

Who Should Attend

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

giac.org

sans.edu

sans.org/cyber-guardian

"Seth's humor keeps getting better as the week goes on, and I'm looking forward to Fri & Sat!"
-Paul Battle, VA Lottery

"This course is giving me a thorough understanding of how web app vulnerabilities can actually be exploited, and therefore why that needed to be fixed."
-Anna Canning, Cannon IT Services LLC

"Course is interactive, fun, intuitive, and educational."
-Glenn Moran, Nordstrom

Seth Misenar *SANS Principal Instructor*

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security 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 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

As a cyber security professional, you have a unique responsibility to find and understand your organization's vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this duty head-on.

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 MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

The whole course is designed to get you ready to conduct a full-scale, high-value penetration test, and on the last day of the course, you'll do just that. After building your skills in awesome labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

You will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. You'll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post exploitation, password attacks, wireless, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

giac.org

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

With comprehensive coverage of tools, techniques, and methodologies for network, web app, and wireless testing, SEC560 truly prepares you to conduct high-value penetration testing projects end-to-end, step-by-step. Every organization needs skilled infosec personnel who can find vulnerabilities and mitigate their impacts, and this whole course is specially designed to get you ready for that role. With over 30 detailed hands-on labs throughout, the course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job masterfully, safely, and efficiently.

sans.edu

sans.org/
cyber-guardian

"This training is valuable because it helps put ideas and concepts into practical application."
-Kajutan Glover, DoD

"This training is extremely important, given the nature of DOD networks, the best answers to compromising a system is likely going to be the hardest to implement."
-David Poulin, 7th Cyber Protection Brigade

Ed Skoudis *SANS Faculty Fellow*

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

SECURITY 566

Implementing and Auditing the Critical Security Controls - In-Depth

SANS

Five-Day Program
Fri, Jan 16 - Tue, Jan 20
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: James Tarala

- GIAC Cert: GCCC
- Masters Program

giac.org

sans.edu

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

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

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

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

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

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

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

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

"This was an awesome course with an amazing amount of material—the capstone did a great job tying it all together."
-D Mayer, Broomfield PD

James Tarala *SANS Senior Instructor*

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

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor:
Christopher Crowley

- GIAC Cert: GMOB
- Masters Program

giac.org

sans.edu

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

"This course was everything I've been looking for over the last few years. Job well done on putting the course together."
-Troy Wojewoda, Huntington Ingalls Industries

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

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient e-mail access as well by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

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

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

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

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From evaluating the network activity generated by mobile applications to mobile code analysis, from exploiting the weaknesses in common mobile applications to conducting a full-scale mobile penetration test, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

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

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Chad Tilbury
- GIAC Cert: GCFE
- Masters Program

digital-forensics.sans.org

Master Computer 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

FOR408: Windows Forensic Analysis focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in 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.

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

"Great course. Great info. Knowledgeable instructor!"
Dan Sorensen, USAF

FOR408 Windows Forensic Analysis will teach you to:

- **Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, XP, and Windows Server 2008/2012**
- **Identify artifact and evidence locations that will answer key questions, including questions about program execution, file opening, external device usage, geo-location, file download, anti-forensics, and system usage**
- **Focus your capabilities on analysis instead of how to use a specific tool**
- **Extract key answers by utilizing proper analysis via a variety of free, open-source, and commercial tools in the Windows SIFT Workstation**

giac.org

sans.edu

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

Chad Tilbury *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Fri, Jan 16 - Wed, Jan 21
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Lenny Zeltser

- GIAC Cert: GREM
- Masters Program

DFIR
digital-forensics.sans.org

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Knowing how to understand capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to understand the inner workings of malicious software and uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. Additionally, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

This course will teach you how to handle self-defending malware, learning to bypass the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts and deobfuscating JavaScript and VBScript to understand the nature of the attack.

You will also learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if it exhibits rootkit characteristics.

The course culminates with a series of capture-the-flag challenges designed to reinforce the techniques learned in class and that provide additional opportunities to learn practical malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

giac.org

sans.edu

"The training is very well documented with lots of hands-on labs; in addition, all topics are discussed thoroughly and reinforced." -Chaz Hobson, Deutsche Bank

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

"Keep up the good work! The instruction and course book enhances learning."
-Israel Sodimu, Veterans Affairs

Lenny Zeltser *SANS Senior Instructor*

Lenny Zeltser is a seasoned business leader with extensive experience in information technology and security. As a product management director at NCR Corporation, he focuses on safeguarding IT infrastructure of small and mid-size businesses world-wide. Before NCR, Lenny led the enterprise security consulting practice at a major IT hosting provider. He also teaches digital forensics and malware courses for the SANS Institute, where he is a senior faculty member. In addition, Lenny is a Board of Directors member at SANS Technology Institute and a volunteer incident handler at the Internet Storm Center. Lenny's expertise is strongest at the intersection of business, technology, and information security practices and includes incident response, cloud services, and product management. He frequently speaks at conferences, writes articles, and has co-authored books on network security and malicious software defenses. Lenny is one of the few individuals in the world who've earned the prestigious GIAC Security Expert designation. He has an MBA degree from MIT Sloan and a Computer Science degree from the University of Pennsylvania. @lennyzeltser

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Fri, Jan 16 - Tue, Jan 20
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: David Hoelzer
Stephen Northcutt

- GIAC Cert: GSLC
- Masters Program
- DoDD 8570

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Who Should Attend

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

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Stephen Northcutt

SANS Faculty Fellow

Stephen Northcutt founded the GIAC certification and served as the founding president of the SANS Technology Institute, an accredited graduate school focused on cyber security. Stephen is author/coauthor of *Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security 2nd Edition, IT Ethics Handbook,* and *Network Intrusion Detection 3rd Edition.* He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer.

giac.org

sans.edu

sans.org/8570

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

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 companies, 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. He 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. @it_audit

SECURITY EAST BONUS SESSIONS

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given by our instructors and selected subject matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: **Stop Giving the Offense an Unfair Advantage** *Dr. Eric Cole*

Recently more and more reports are coming out stating that the offense has an advantage. This is confirmed by the increase in attacks and the number of organizations that are being compromised. However, it does not have to be this way. The reason the offense has the advantage is that the defense gave it to them. Many organizations spend a significant amount of money on cyber security, but they are not focusing in on the right areas. By understanding how the offense works, organizations can build security solutions that take the advantage away from the offense and give it back to the defense. In this engaging talk, Dr. Cole will discuss actionable items taken directly out of SEC401: Security Essentials that show how to build a defendable network. Find out what the top organizations are doing to properly protect their organizations.

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.

Enterprise PowerShell for Remote Security Assessment *James Tarala*

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Not only are organizations attempting to automate their assessments, the need is becoming more pressing to perform assessments centrally against large numbers of enterprise systems. Forensic analysts, incident handlers, penetration testers, and auditors all regularly find themselves in situations where they need to remotely assess a large number of systems through an automated set of tools. Microsoft's PowerShell scripting language has become the defacto standard for many organizations looking to perform this level of distributed automation. In this presentation James Tarala, of Enclave Security, will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large scale Windows security assessments.

What Malware? Hunting Command Line Activity *Chad Tilbury*

There is a reason hackers use the command line, and it isn't to impress you with their prowess. Throughout the history of Windows, the command line has left far fewer forensic artifacts than equivalent operations via the GUI. To make matters worse, the transition to Windows 7 and 8 has spread PowerShell throughout the enterprise. While it makes our lives easier as defenders, it does the same for our adversaries. Every time you marvel at the capabilities of PowerShell, you should fear how your adversaries may use that power against you. We will show how incident responders are countering the command line threat via real-world examples. Learn to identify when it is in play, extract commands from memory and network packets, and see what is new on the horizon from Microsoft to make tracking command line activity easier.

Evolving Threats *Paul A. Henry*

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

SECURITY EAST BONUS SESSIONS

CONTINUED

Gone in 60 Minutes: Have You Patched Your System Today? *David Hoelzer*

In our industry we hear about new vulnerabilities every day, but there can be a perception that moving from the discovery of a flaw to a workable exploit is very difficult. The result is that most organizations are perfectly happy operating with a 30-day patch-rollout cycle. Is this really fast enough? How hard is it really to exploit a vulnerability? How hard is it to scale a proof of concept into a working tool that can compromise thousands of hosts? This presentation demonstrates the entire process, walking through the process that a security researcher or hacker follows from research through proof of concept and working exploit... all in less than 60 minutes. While aspects of this presentation can be somewhat technical, the emphasis isn't on the technical but on the process and speed with which a working exploit can be developed. There's something for everyone to take away from this presentation!

Client Access is the Achilles' Heel of the Cloud *Bryce Galbraith*

Representations of cloud infrastructures often reassure us of their robust security mechanisms by prominently displaying the familiar gold lock in the center of the cloud. While many cloud providers genuinely do strive to deliver confidentiality, integrity, and availability the vital question remains, "Is our data actually secure or not?" The truth is, our data is vulnerable virtually everywhere except the cloud (assuming it is secure there to begin with). Client access is the Achilles' heel of the cloud. Live attack demonstrations will clearly illustrate how virtually all security controls provided by the cloud can be circumvented and the data held within can be accessed by attackers. If you are serious about protecting your data, wherever it goes, you will want to be keenly aware of these risks.

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)**

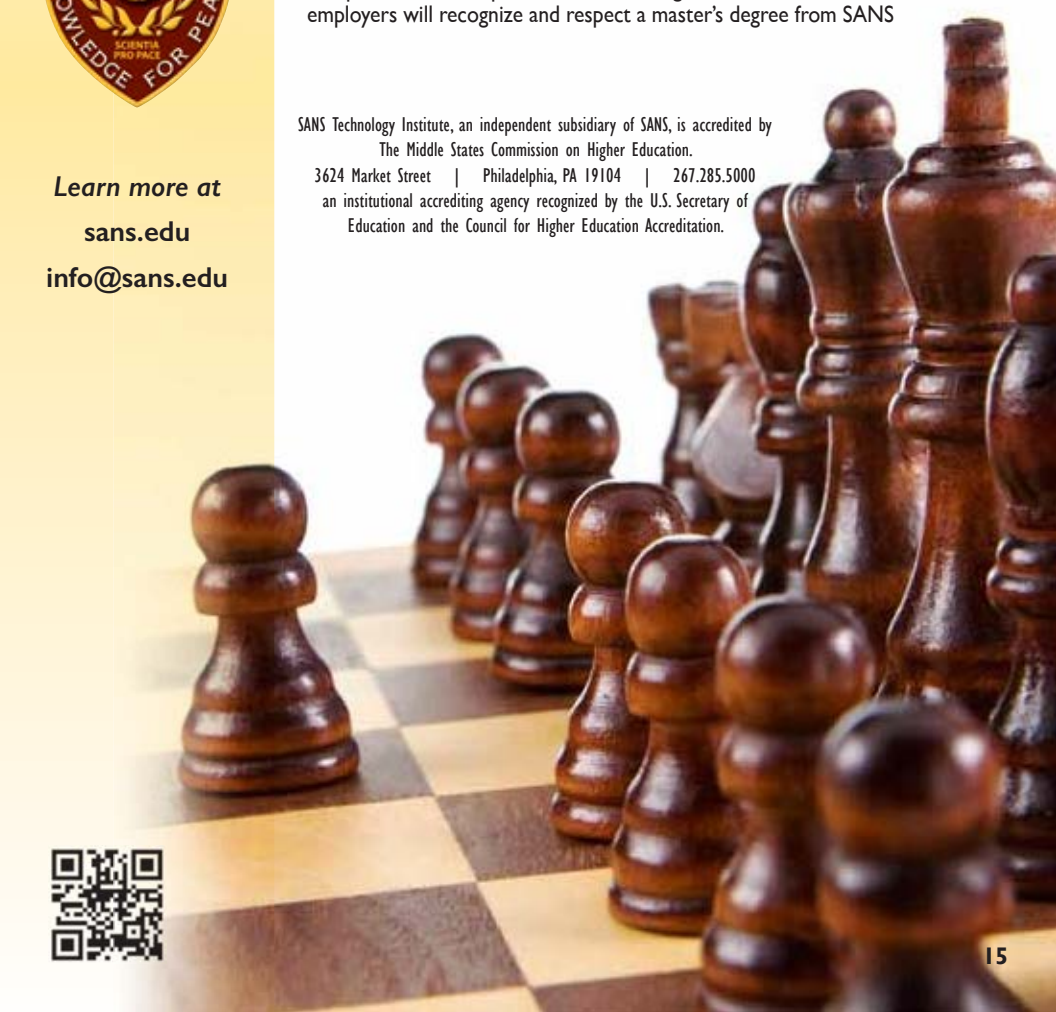
Top Reasons Students Choose SANS Graduate Programs:

- 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

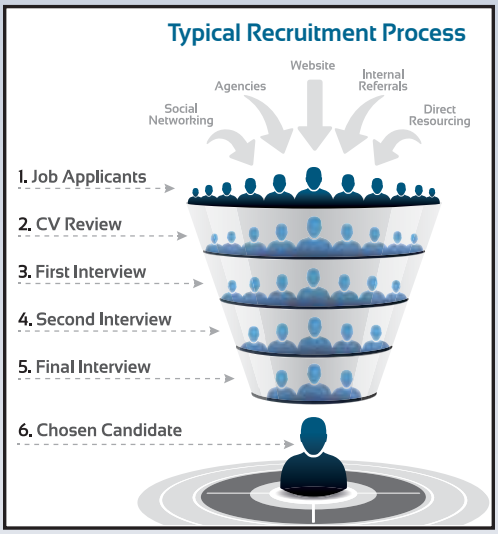
SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education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



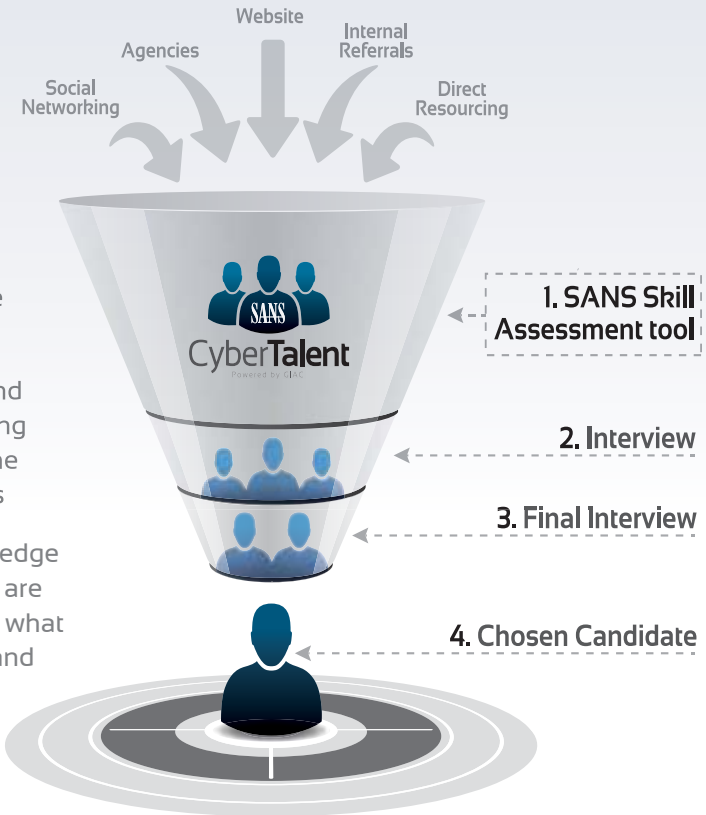
SANS CyberTalent
Powered by GIAC

How SANS CyberTalent Assessments Work

SANS CyberTalent is a web-based skills evaluation tool that enables hiring managers and recruiters to accurately gauge the skillset of information security job applicants and current staff. 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 cyber security team.



Future Recruitment Process



Using the SANS Skills Assessment tool will have the following results:

1. Greatly increase the candidate pool
2. Reduce interview and admin time by cutting out two stages of the recruitment process
3. Provide clear knowledge that the people you are interviewing can do what they say they can (and sometimes more!)

SANS CYBER GUARDIAN PROGRAM

sans.org/cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

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

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

Program Prerequisites

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

Core Courses

SEC503 Intrusion Detection In-Depth (GCIA)

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling (GCIH)

SEC560 Network Penetration Testing and Ethical Hacking (GPEN)

FOR508 Advanced Computer Forensic Analysis and Incident Response (GCFA)

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

Blue Team Courses

SEC502 Perimeter Protection In-Depth (GPPA)

SEC505 Securing Windows with the Critical Security Controls (GCWN)

SEC506 Securing Linux/Unix (GCUX)

Red Team Courses

SEC542 Web App Penetration Testing and Ethical Hacking (GWAPT)

SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)

SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (GXPN)

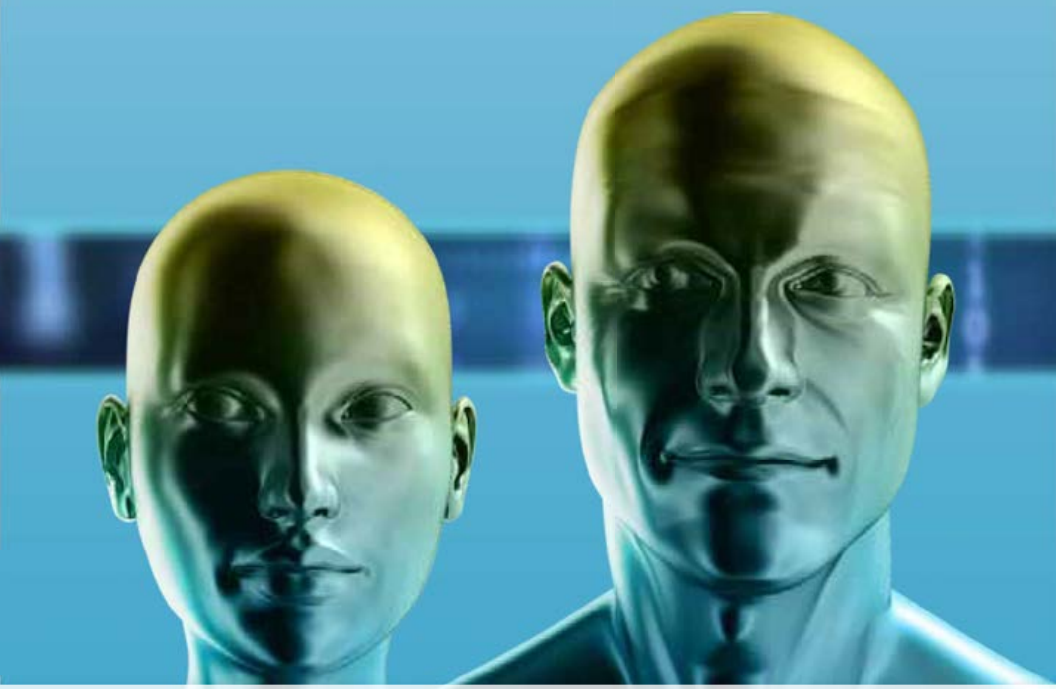
The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Healthcare - 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.
  - STH.Healthcare focuses on security behaviors for individuals who interact with Protected Health Information (PHI).
  - 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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

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

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

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

sans.org/community

OnSite

Live Training at Your Office Location

sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

sans.org/mentor

Summit

Live IT Security Summits and Training

sans.org/summit

ONLINE TRAINING

OnDemand

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

sans.org/ondemand

vLive

Online, Evening Courses with SANS' Top Instructors

sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

sans.org/simulcast

OnDemand Bundles

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

FUTURE SANS TRAINING EVENTS

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

SANS Cyber Defense San Diego 2014

San Diego, CA | November 3-8

SANS DFIRCON East 2014

Fort Lauderdale, FL | November 3-8

SANS Pen Test Hackfest 2014

Washington, DC | November 13-20

Healthcare Cyber Security SUMMIT & TRAINING 2014

San Francisco, CA | December 3-10

SANS Cyber Defense Initiative 2014

Washington, DC | December 10-19

Cyber Threat Intelligence SUMMIT & TRAINING 2015

Washington, DC | February 2-9

SANS Scottsdale 2015

Scottsdale, AZ | February 16-21

ICS Security – Orlando SUMMIT & TRAINING 2015

Orlando, FL | February 23 – March 2

SANS SECURITY EAST 2015

Hotel Information

Training Campus
Hilton New Orleans Riverside

Two Poydras Street
New Orleans, LA 70130
sans.org/event/security-east-2015/location

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

Special Hotel Rates Available

A special discounted rate of $199.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high speed Internet in your room and are only available through December 22, 2014. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

Top 5 reasons to stay at the Hilton New Orleans Riverside

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Hilton New Orleans Riverside, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Hilton New Orleans Riverside that you won't want to miss!
5. Everything is in one convenient location!

SANS SECURITY EAST 2015

Registration Information

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

Register online at sans.org/event/security-east-2015/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	11/26/14	$400.00	12/17/14	$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)*

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

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

**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 December 24, 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