THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS San Diego 2013

San Diego, CA | November 18-23

Choose from these popular courses:

Securing Windows and Resisting Malware ***NEW!***

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

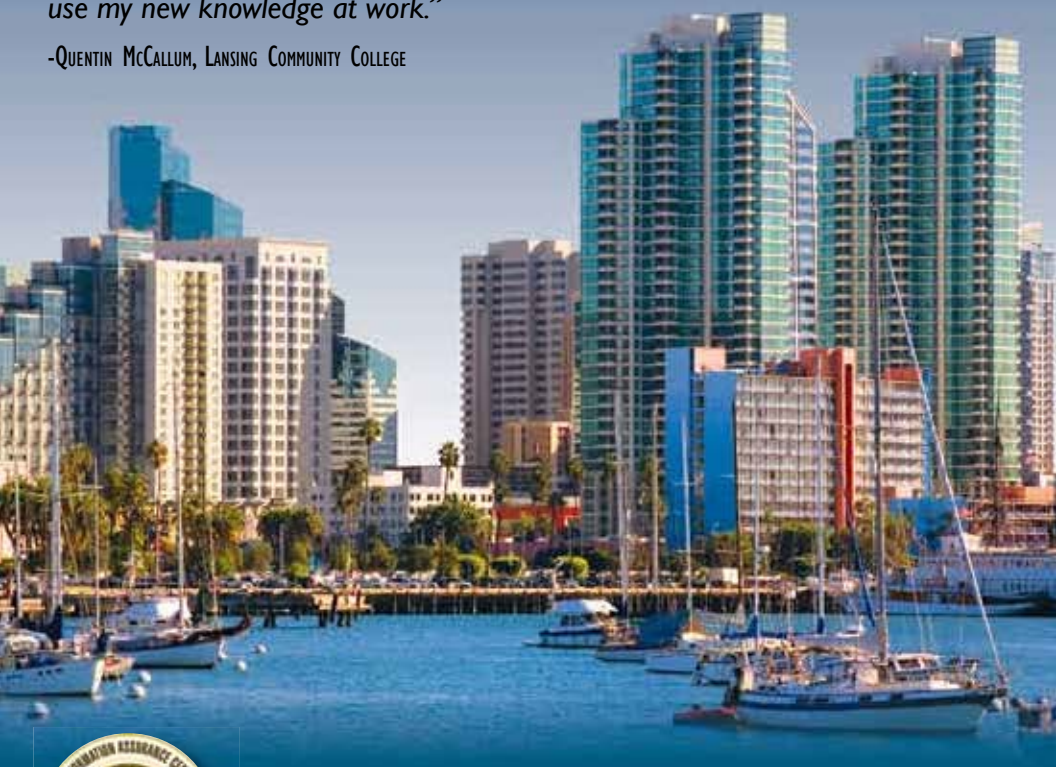
Network Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

Advanced Computer Forensic Analysis and Incident Response

"Exceeded my expectations for content and practicality. I will be able to immediately use my new knowledge at work."

-Quentin McCallum, Lansing Community College



GIAC Approved Training

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

Save $500 by registering early!

See page 13 for more details.

We are pleased to invite you to **SANS San Diego 2013 on November 18-23 located at the Hard Rock Hotel!** Don't miss the chance for a late fall trip to Southern California for our courses in IT security, pen testing, computer forensic analysis, and our new **SEC505 Securing Windows and Resisting Malware** course. You will return home with valuable, hands-on experience, and security skills!

Our hand-picked instructors have real-world experience, and are experts in their field, so what you learn in the classroom will be up-to-date and relevant to your job. See this brochure for a complete schedule, course descriptions, instructor bios, GIAC cert availability for all of our courses, and information about earning your Master's Degree in Information Security through the SANS Technology Institute (STI). Don't miss our timely bonus evening talks presented by SANS' top instructors. These special presentations are free to everyone who takes a course.

The Hard Rock Hotel San Diego is located in the city's Gaslamp Quarter across the street from the San Diego Convention Center. From the website for the hotel: "Experience the distinctive brand of rock star-style glamour celebrated only at Hard Rock Hotel San Diego. Not only will our unconventionally sleek and contemporary design wow you, but our unique amenities and expectation-exceeding service will provide you with an authentic experience that simply rocks!" See our Hotel and Travel Information (page 13) for more details.

San Diego is an awesome destination with November average temps reaching 70 degrees. There are so many things to do, and here are a few things that are happening during the week of SANS San Diego 2013:

- **Tour the elegant Hotel del Coronado & the Historic Coronado –** Coronado Visitor Center and Historical Association & Museum, location: Coronado Island
- **New! 3D/4D Theater and Interactive Air and Space Technology Kid Zone –** San Diego Air and Space Museum, location: Balboa Park
- **Tour Balboa Parks spectacular gardens open 24 hours a day –** location: Balboa Park
- **Visit Cabrillo National Monument for breathtaking views of San Diego –** location: San Diego National Park
- **10th Annual San Diego Bay Wine & Food Festival –** November 20-24
- **SeaWorld's Christmas Celebration, SeaWorld San Diego –** Starting November 16, location: Mission Bay
- **Dr. Seuss' "How the Grinch Stole Christmas!" –** November-December, location: Balboa Park

You won't want to miss SANS San Diego 2013 where you can experience the very best security training. **Register and pay by Wednesday, October 2, to receive a $500.00 discount.** Start making your training and travel plans now and let your colleagues and friends know about SANS San Diego 2013. We look forward to seeing you there!

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

"My favorite time of year is when SANS comes to town."
-Mike Chandler, Southern California Edison

"I can make effective use of 100% of the things I've learned! As I stated previously, I'm certain that I can pay for this course, twice over, with the tools and techniques that I've learned! Great class, great instructors... looking forward to my next SANS course!"
-Wes Akers, RockTennCompany

"This course has a very good mix of the theoretical and the practical. Great course – my first SANS class. I am going to take the exam, and I will be back for more."
-Kevin Wixted, DLA Piper LLP

"Awesome content, great instructor, and support staff."
-Purnima Mysore, Qualcomm

Courses-at-a-Glance

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Nov 18 - Sat, Nov 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Keith Palmgren

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

Who Should Attend

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

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.

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

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

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared 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 gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

www.giac.org

www.sans.edu

"I'm a newbie to security. This course presented a ton of information on this subject in a fast-paced, easy-to-understand manner."
-Michael Horkan, Rockwell Automation

www.sans.org/
cyber-guardian


www.sans.org/8570

Keith Palmgren *SANS Certified Instructor*

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

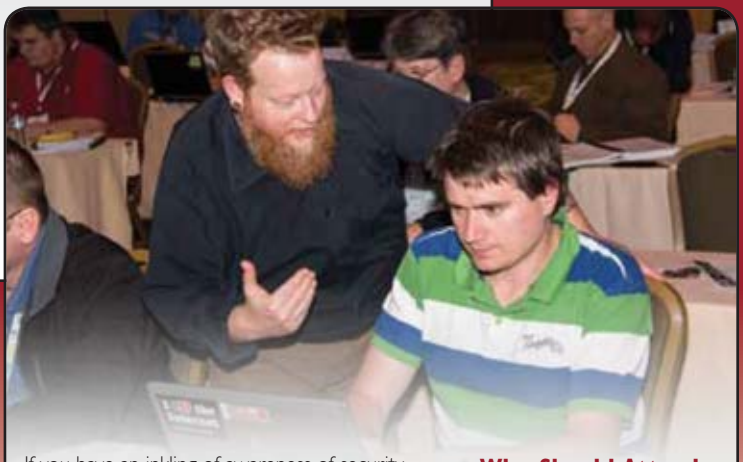
SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Nov 18 - Sat, Nov 23
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor

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



"Intrusion Detection is vital for Security administrations. This helps us to be proactive in identifying security threats."
-Sukhwinder, Accenture

"Intrusion detection skills are a must-have for technical security professionals and this course gives us the knowledge to be successful."
-Josh Johnson,
Wegmans Food Markets

"There is information in SEC503 that I have never seen before in my 17 years in IT."
-Jesse Trucks, ORNL

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

Who Should Attend

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

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

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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

Mike Poor *SANS Senior Instructor*

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

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Nov 18 - Sat, Nov 23
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Seth Misenar

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

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

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

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

Who Should Attend

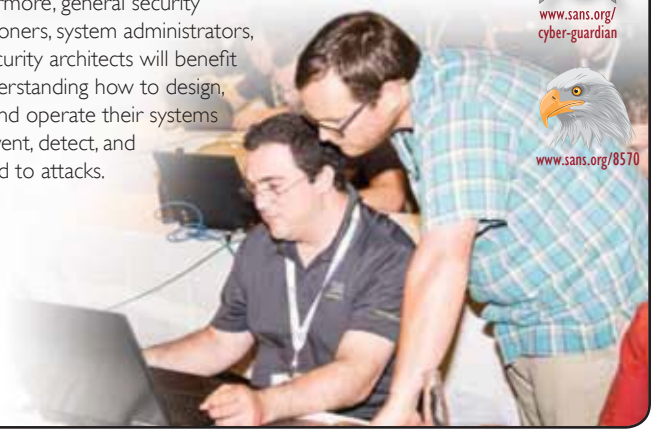
- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570



"This class should be required for all security personnel because it really gives you a functional understanding of the security dangers we read about every day."
-Joe Rudich, Blue Cross Blue Shield of Minnesota

"This class teaches you all of the hacking techniques that you need as an incident handler."
-Demonique Lewis, TerpSys

Seth Misenar *SANS Certified Instructor*

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security 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. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including SEC401: SANS Security Essentials Bootcamp Style, SEC504: Hacker Techniques, Exploits, and Incident Handling, and SEC542: Web App Penetration Testing and Ethical Hacking. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute.

SECURITY 505

Securing Windows and Resisting Malware

NEW

Six-Day Program
Mon, Nov 18 - Sat, Nov 23
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Masters Program
- Cyber Guardian

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The **Securing Windows and Resisting Malware** course is fully updated for Windows Server 2012, Windows 8, Server 2008-R2, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact on users of these changes. You'll see the instructor demo the important steps live, and, if you bring a laptop, you can follow along too. The manuals are filled with screenshots and step-by-step exercises, so you can do the steps alongside the instructor in seminar or later on your own time if you prefer.

We've all got anti-virus scanners, but what else needs to be done to combat malware and intruders using Advanced Persistent Threat (APT) techniques? Today's weapon of choice for hackers is stealthy malware with remote control channels, preferably with autonomous worm capabilities, installed through client-side exploits. While other courses focus on detection or remediation, the goal of this course is to prevent the infection in the first place (after all, first things first).

Especially in Server 2012 and beyond, PowerShell dominates Windows scripting and automation. It seems everything can be managed through PowerShell now. And if there's a needed skill that will most benefit the career of a Windows specialist, it's being able to write PowerShell scripts, because most of your competition will lack scripting skills, so it's a great way to make your resume stand out. This course devotes an entire day to PowerShell scripting, but you don't need any prior scripting experience.

Who Should Attend

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

"If you think you know Windows, take this Windows security course. As you review your skills and understanding, you will be challenged for the better!!"
-Matthew Stoeckle, Nebraska Public Power District

"SEC505 has a direct impact on Windows OS security and is a must for any sys admin in this day and age."
-Chris Linville, Raytheon

"All I will say is that this is the best Microsoft training that I've received. I will recommend this training to my peers. More power to SANS!"
-Ceferino Aratea, Jr., NAVAIR

Jason Fossen *SANS Faculty Fellow*

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

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Nov 18 - Sat, Nov 23
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

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

Who Should Attend

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

"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend."
-Mark Hamilton, McAfee

"The skills taught and demonstrated in this class are perfect for new pen testers and veterans alike."
-Roy Luongo, Dept of Defense

"Capture The Flag. Stellar real-world experience."
-Russell Swift Princess Cruises

Equipping Security Organizations with Advanced Penetration Testing and Ethical Hacking Know-How

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. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. 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. The final portion of the class includes a comprehensive hands-on exercise, conducting a penetration test against a hypothetical target organization, following all of the steps.

www.giac.org

www.sans.edu

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

www.sans.org/
cyber-guardian

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, 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.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

SANS

Six-Day Program
Mon, Nov 18 - Sat, Nov 23
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Alissa Torres

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

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

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?

The updated FOR508 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.

"This was a great course, it taught me things that can be used back in the office right away. I really enjoyed FOR508. Alissa is a great instructor and added energy to the course. I'm looking forward to practicing the techniques from this course."
-Lisa Smith, BEA

Who Should Attend

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

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

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+.

SAN DIEGO 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: Windows Exploratory Surgery with Process Hacker *Jason Fossen*

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware. **http://processhacker.sourceforge.net**

Introducing the CompTIA® CASP™ Exam *Seth Misenar*

Seth Misenar, coauthor of *Syngress CISSP Study Guide* with Eric Conrad, will introduce you to the new CompTIA® Advanced Security Practitioner certification, a hands-on technical exam with a mix of deeper technical questions, as well as higher-level management questions. The CASP™ was recently added to DoD 8570 for the following roles: IAT level III, IAM II, and IASAE level I and II. Will this cert be a valuable addition to your resume? Will this cert bleed significant market share from the CISSP®? Now that it has been added to DoD8570, will CASP™ become the go to DoD cert? Come find out where CASP™ fits into the security certification landscape and see if Eric and Seth's new SANS prep course for the CASP™ is right for you.

SANS 8 Mobile Device Security Steps *Chris Crowley*

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

Who's Watching the Watchers? *Mike Poor*

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

Identifying Today's Top 5 Lateral Movement Techniques *Alissa Torres*

In order to properly scope an incident and identify all of the systems involved, a responder must be able to detect signs of lateral movement. Yet, today's attackers are developing more sophisticated techniques of traversing the network, leaving behind minimal footprints through the use of PowerShell and WMIC queries and remote executions. During this presentation, attendees will be introduced to the top 5 current lateral movement techniques, as well as armed with techniques for their detection.

GIAC Program Overview

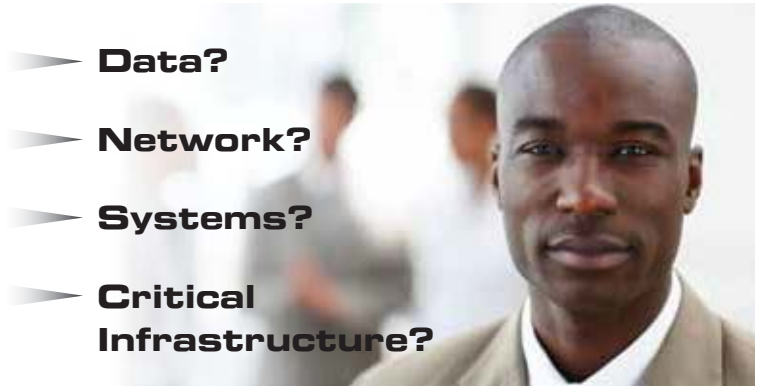
SANS Technology Institute Open House

Vendor Showcase

Tuesday, November 19 | 10:30am-10:50am | 12:30pm-1:15pm | 3:00pm-3:20pm

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

How Are You Protecting Your



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

Get GIAC certified!

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

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

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

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

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

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Techniques, Exploits, and Incident Handling	GCIH
AUD507	Auditing Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	GSLC

Compliance/Recertification:

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

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

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

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

STI offers two unique master's degree programs:

Master of Science in Information Security Engineering

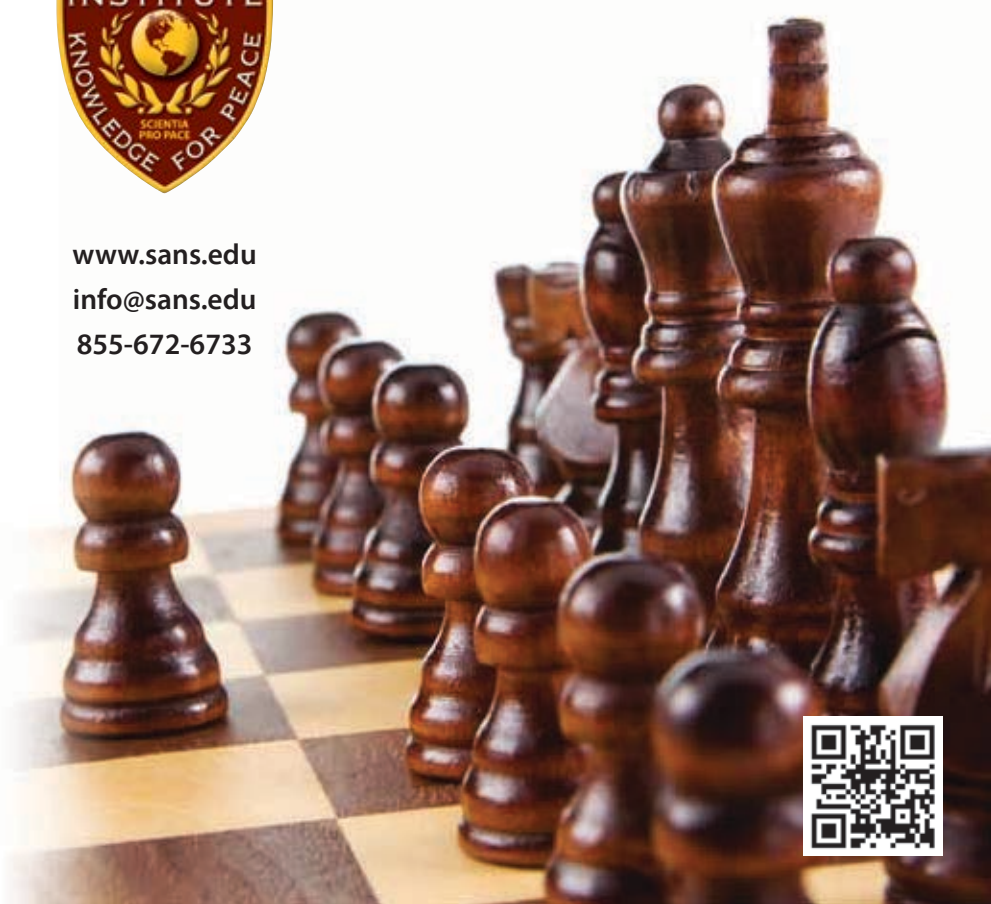
Master of Science in Information Security Management

"The STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience - you walk out of every class with skills you can use immediately."

-Courtney Imbert, MSISE Student

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

www.sans.edu
info@sans.edu
855-672-6733



SANS
CYBER GUARDIAN
PROGRAM

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

Real Threats
Real Skills
Real Success

Join Today!

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

www.sans.org/cyber-guardian

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)

SECURITY AWARENESS
FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPPA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org

FUTURE SANS TRAINING EVENTS

SANS CyberCon Fall 2013

Online Training | September 9-14

www.sans.org/cybercon

SANS Network Security 2013

Las Vegas, NV | September 14-23

www.sans.org/event/network-security-2013

SANS Seattle 2013

Seattle, WA | October 7-14

www.sans.org/event/seattle-2013

SANS Baltimore 2013

Baltimore, MD | October 14-19

www.sans.org/event/baltimore-2013

SANS Chicago 2013

Chicago, IL | Oct 28 - Nov 2

www.sans.org/event/chicago-2013

SANS South Florida 2013

Fort Lauderdale, FL | November 4-9

www.sans.org/event/south-florida-2013

SANS Pen Test Hackfest
TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

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

SANS San Antonio 2013

San Antonio, TX | December 3-8

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

SANS Cyber Defense Initiative 2013

Washington, DC | December 12-19

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

SANS TRAINING FORMATS

LIVE CLASSROM 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 SAN DIEGO 2013

Hotel Information

Training Campus
Hard Rock Hotel

207 Fifth Avenue
San Diego, CA 92101
www.sans.org/event/san-diego-2013/location

Special Hotel Rates Available

A special discounted rate of $210.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through October 19, 2013. To make reservations please call (866) 751-ROCK (866-751-7665) and ask for the SANS November 2013 group rate.

The Hard Rock Hotel San Diego is a Four-Diamond property, with a design, amenities, and vibe infused with the passion and irreverence of Rock 'n' Roll. Its location is one of the most coveted among downtown San Diego hotels – right at the entrance to the Gaslamp Quarter, by the San Diego Convention Center and PETCO Park. Whether you're coming to the city for business or pleasure, the Hard Rock will give you an authentic experience that rocks!

Top 5 reasons to stay at the Hard Rock Hotel

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 Hard Rock Hotel, 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 Hard Rock Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN DIEGO 2013

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/san-diego-2013

To register, go to www.sans.org/event/san-diego-2013

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 **October 23, 2013** – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	10/2/13	$500.00	10/16/13	$250.00

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 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.

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