SANS South Florida 2013

Fort Lauderdale, FL | November 4-9

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Computer Forensic Investigations – Windows In-Depth

Defending Web Applications Security Essentials

"The instructor provided great real-world examples to reinforce the subject matter."

-Michael Hulin, Coventry Health Care

GIAC Approved Training

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

Save $500 by registering early!

See page 13 for more details.

Dear Colleague,

Allow me to invite you to our first **SANS South Florida 2013** training event. We will be at the **Westin Fort Lauderdale** campus on **November 4-9**. Improve your skills by taking advantage of this hands-on training, presented by security industry leaders, Dr. Eric Cole, Dr. Johannes Ullrich, Paul A. Henry, Eric Conrad, and Michael Murr. They will ensure that you not only learn the material, but that you can also apply it immediately when you return to the office. You'll see why SANS is the most trusted source in computer security training, certification, and research.

Henri van Goethem

Please take the time to look through the brochure to learn about our evening events and talks that enhance your training. This brochure will walk you through course descriptions and instructor bios. You will find information about the *GIAC Certifications* that you can earn in addition to your training. All five of our courses offered at SANS South Florida 2013 are associated with a *GIAC Certification* and SEC401 and SEC504 are aligned with *DoD Directive 8570*. And all five our offerings will help you earn your Master's Degree at SANS Technology Institute (STI). This brochure will provide you with information about why you should apply!

Note that you can attend all courses at this event remotely if you are unable to travel. *Event Simulcast* allows you to attend a SANS training event without leaving home. Simply log in to a virtual classroom to see, hear, and participate in the class as it is being presented LIVE at the event.

Our campus, Westin Fort Lauderdale, is located in warm, sunny Fort Lauderdale/ Pompano Beach. South Florida is a fabulous destination for training with all that there is to do. The temperature in Fort Lauderdale in November is between 66 degrees and 81 degrees, so it's all about the beach! Enjoy these clean, safe, user-friendly Florida beaches: Hollywood, Dania Beach, Deerfield Beach, Pompano Beach, Lauderdale-by-the-Sea, and Fort Lauderdale.

A special discounted rate of $129 Single/Double will be honored at the Westin Fort Lauderdale based on space availability, and this rate includes high-speed Internet in your room. Government per diem rooms are available with proper ID; you must call the hotel and specifically ask for this rate. Make your reservations now, as this special rate is only available through October 12, 2013.

Receive a discount of up to $500 for any full course paid for by Wednesday, September 18, 2013!

"I have attended many conferences, SANS training events are well above the rest." says Kenton Groombridge, US Army. Come see for yourself – register today for SANS South Florida 2013.

Kind Regards,

Henri van Goethem
Henri van Goethem
Director of Forensics and Pen Test Curricula

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

"Fantastic class! Fantastic Instructor! I have taken six SANS classes and I haven't had a bad experience yet. They are just so professionally done!"
-Tom Cook, United States Military Academy

"I learn something new every conference. What you learn does apply to work and does work."
-David Fava, Boeing

"Excellent information that I will be able to quickly apply back in the office."
-Gregory Fellin, UC Merced

Courses-at-a-Glance

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, Nov 4 – Sat, Nov 9
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

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 not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. 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 and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore we will teach you how 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.

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, auditors who need a solid foundation of security principles so they can be effective as possible at their jobs**
- **Anyone new to information security with some background in information systems and networking**

With the APT (advanced persistent threat), 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.

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including ***Advanced Persistent Threat***, ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible*** 2nd Edition, 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 the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/south-florida-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

DoDD 8570 Required
www.sans.org/8570

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Nov 4 – Sat, Nov 9
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
Laptop Required • 37 CPE/CMU Credits
Instructor: Eric Conrad

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.

Simulcast
Attend remotely via Simulcast
See page 7 for more info.

"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."
-Joshua Anthony, West Virginia Army National Guard

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, 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.

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

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.

"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."
-Anthony Liu, Scotia Bank

"The lab was challenging and forced out-of-the-box thinking."
-Rafael Cabrera, Air Force

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/south-florida-2013.

GIAC CERTIFIED INCIDENT HANDLER GCIH
www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

DoDD 8570 Required
www.sans.org/8570

Eric Conrad *SANS Certified Instructor*

Eric Conrad is lead author of the book ***The CISSP Study Guide***. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at **www.ericconrad.com**.

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Nov 4 – Sat, Nov 9
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
Laptop Required • 37 CPE/CMU Credits
Instructor: Michael Murr

Simulcast
Attend remotely via Simulcast
See page 7 for more info.

"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

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.

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.

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**

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.

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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/south-florida-2013.

GIAC CERTIFIED PENETRATION TESTER GPEN
www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
www.sans.edu

supere aude
www.sans.org/cyber-guardian

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about Digital forensics on his Forensic Computing blog. **www.forensicblog.org**

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Nov 4 – Sat, Nov 9
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Paul A. Henry

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threats, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and calling in cybercrime law enforcement agents to piece together what happened in these cases.

FOR408: Computer Forensic Investigations – Windows In-Depth focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008) you will be exposed to well known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that students can take with them.

Simulcast
Attend remotely via Simulcast
See page 7 for more info.

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/south-florida-2013.

What you will receive with this course

- **Windows version of the SIFT Workstation Virtual Machine**
- **Windows 8 Standard Full Version License and Key for the Windows SIFT Workstation**
- **Full License to AccessData FTK and Guidance Software EnCase for a 3 month trial**
- **Full License to MagnetForensics Internet Evidence Finder for a 15 day trial**
- **Two full real-world cases to examine during class**
- **Course DVD loaded with case examples, tools, and documentation**
- **Wiebetech Ultradock v5 Write Blocker Kit**

"Hands down the BEST forensics class EVER!! Blew my mind at least once a day for 6 days!" -Jason Jones, USAF

"FOR408 is absolutely necessary for any computer forensic type career. Excellent information!" -Rebecca Passmore, FBI

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

DFIR
http://computer-forensics.sans.org

GCFE
www.giac.org

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

DEVELOPER 522

Defending Web Applications Security Essentials

Six-Day Program • Mon, Nov 4 – Sat, Nov 9
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dr. Johannes Ullrich

This is the course to take if you have to defend web applications!

Simulcast
Attend remotely via Simulcast
See page 7 for more info.

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

"What you don't know about web app defense is most likely killing you and you wouldn't know it."
-Michael Malarkey, Bank of America

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and infrastructure security professionals who have an interest in better defending their web applications.

Who Should Attend:

- **Application developers**
- **Application security analysts or managers**
- **Application architects**
- **Penetration testers who are interested in learning about defensive strategies**
- **Security professionals who are interested in learning about web application security**
- **Auditors who need to understand defensive mechanisms in web applications**
- **Employees of PCI compliant organizations who need to be trained to comply with PCI requirements**

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. The topics that will be covered include:

- **Infrastructure Security**
- **Server Configuration**
- **Authentication mechanisms**
- **Application language configuration**
- **Cross-Site Request Forging**
- **Application coding errors like SQL Injection and Cross-Site Scripting**
- **Authentication Bypass**
- **Web services and related flaws**
- **Business logic flaws**
- **Web 2.0 and its use of web services**
- **XPATH and XQUERY languages and injection**
- **Protective HTTP Headers**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/south-florida-2013.

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

Dr. Johannes Ullrich *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. Prior to working for SANS, Johannes worked as a lead support engineer for a Web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also maintains a daily security news summary podcast (**http://isc.sans.edu/podcast.html**) and enjoys blogging about application security (**http://software-security.sans.org/blog**).

GIAC CERTIFIED WEB APPLICATION DEFENDER GWEB
www.giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
www.sans.edu

South Florida Bonus Sessions

SANS@Night Evening Talks

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

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

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act.

In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

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 6 years.

The Security Impact of IPv6 *Dr. Johannes Ullrich*

IPv6 is more then just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the "DC" to "AC" conversion in the electric world. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocol's opportunities are not well understood, and IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody's pet.

GIAC Program Overview

GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. Find out why this is important to your career.

SANS Technology Institute Open House

SANS Technology Institute Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers: management skills and technical mastery. If you aspire to help lead your organization's or your country's information security program and you have the qualifications, organizational backing, and personal drive to excel in these challenging degree programs, we will welcome you into the program.

You don't have to miss out on SANS' top-rated training. Attend any SANS South Florida 2013 course remotely via SANS Simulcast!

How SANS Simulcast Works

Cutting-edge webcast technology and live instruction combine to deliver a fun and engaging remote learning experience. Remote students will also receive four months of access to an archived copy of the class to use as a reference tool or to catch up on a missed session. The platform is web-based so students simply need a solid internet connection to participate.

"This is the first web-based training course I have done and was wondering if it would actually be worthwhile. It surpassed my expectations! The software and technology worked really well, the presenter kept everything moving along nicely and was quick to pick up on participants' comments during the lecture segments. The IM component adds value – lots of good information/comments from the class."

-Jeremy Gay, Montana State University

The following courses will be available via SANS Simulcast:

SEC401

SEC504

SEC560

FOR408

DEV522

SANS Event Simulcast classes are:

COST-EFFECTIVE – You can save thousands of dollars on travel costs, making Event Simulcast an ideal solution for students working with limited training budgets or travel bans.

ENGAGING – Event Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.

CONDENSED – Complete your course quickly; all SANS Event Simulcast classes take no longer than six days to complete.

REPEATABLE – Event Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.

COMPLETE – You will receive the same books, discs, and MP3 audio files that conference students receive, and you will see and hear the same information as it is presented at the live event.

To register for a SANS South Florida 2013 Simulcast course, please visit www.sans.org/event/south-florida-2013/attend-remotely

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

"A degree is great. A graduate degree plus current actionable knowledge is even better. STI provides this and more."
-Seth Misenar, MSISE Student

Apply today!
New cohorts are forming now.
www.sans.edu

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

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

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 & 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

SANS
CYBER GUARDIAN
PROGRAM

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

Real Threats
Real Skills
Real Success

Prerequisites

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

Core Courses

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

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

Blue Team Courses

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

Red Team Courses

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

Join Today!

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

www.sans.org/cyber-guardian

SECURITY AWARENESS
FOR THE 21st CENTURY

SANS SECURING THE HUMAN END USER
SANS SECURING THE HUMAN UTILITY
SANS SECURING THE HUMAN DEVELOPER
SANS SECURING THE HUMAN PHISHING

- 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 **Capital City** 2013

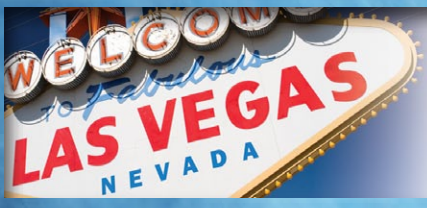
Washington, DC | September 3-8

www.sans.org/event/sans-capital-city-2013

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 **Pen Test Hackfest** TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

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

SANS **San Diego** 2013

San Diego, CA | November 18-23

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

SANS **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 South Florida 2013

Hotel Information

Training Campus
Westin Fort Lauderdale

400 Corporate Drive
Fort Lauderdale, FL 33334
www.sans.org/event/south-florida-2013/location

Special Hotel Rates Available

A special discounted rate of $129.00 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 12, 2013. To make reservations please call (800) 937-8461 and ask for the SANS group rate.

The Westin Fort Lauderdale is located in the warm Fort Lauderdale/Pompano Beach sun overlooking a beautiful three-acre tropical lagoon, and is awaiting your arrival. The guest rooms are newly remodeled, including the second generation Heavenly Bed (SM) and invigorating Heavenly Bath®.

Top 5 reasons to stay at the Westin Fort Lauderdale

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 Westin Fort Lauderdale, 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 Westin Fort Lauderdale that you won't want to miss!
5. Everything is in one convenient location!

SANS South Florida 2013

Registration Information

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

To register, go to
www.sans.org/event/south-florida-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 9, 2013 – processing fees may apply.

To register for a SANS South Florida 2013 Simulcast course, please visit www.sans.org/event/south-florida-2013/attend-remotely

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	9/18/13	$500.00	10/2/13	$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