THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Boston 2014

Boston, MA July 28 - August 2

Choose from these popular courses:

Advanced Network Forensics and Analysis **NEW!**

Advanced Smartphone Forensics **NEW!**

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Windows Forensic Analysis

Web App Penetration Testing and Ethical Hacking

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

Advanced Security Essentials - Enterprise Defender

Mobile Device Security and Ethical Hacking

Defending Web Applications Security Essentials

Save $400 by registering early!
See page 17 for more details.

*"Take it from an info security professional,
if you want to learn how to do it the right way, go to SANS."*
-Tony Robinson, Ft Meade DoD

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

GIAC Approved Training

Please join us in Boston this summer for one of SANS' best line-ups in cutting-edge cybersecurity training July 28 – August 2! Don't miss the chance to gain in-depth knowledge that is the best investment for security training courses that you can make. This SANS training event is full of important and immediately useful techniques that you can put to work as soon as you return to your office. We will be offering two new forensic courses ***FOR572: Advanced Network Forensics and Analysis*** taught by Philip Hagen and ***FOR585: Advanced Smartphone Forensics*** taught by Cindy Murphy along with nine more six-day courses in security management, IT and mobile security, computer forensics, and web applications security.

SANS Boston 2014 offers top-rated courses brought to you by Dr. Eric Cole, Jason Fossen, Rob Lee, Johannes Ullrich, Ph.D., George Bakos, Eric Conrad, Christopher Crowley, Ted Demopoulos, Seth Misenar, Philip Hagen, and Cindy Murphy. This team helped SANS to be named ***Best Professional Training*** by *SC Magazine* for 2014. See instructor bios and course descriptions inside. Nine courses are associated with the prestigious ***GIAC Certification***. If you want to fast track your career, check which courses may help you earn your Master's Degree at the ***SANS Technology Institute*** (STI). Find out about GIAC and STI in this brochure. Also, look for details about our ***Vendor Showcase*** (July 30) along with a tremendous lineup of ***SANS@Night*** evening events. These extra sessions are free with your paid tuition and are a great enhancement to your training.

Come to Boston to learn from SANS and soak in the great historic culture of this fascinating city. Our campus will be at the ***Hilton Boston Back Bay*** hotel, which is just five blocks from the Boston Common where the starting point of the Freedom Trail begins. Some of Boston's top must-see sights and attractions are the Freedom Trail, Boston Public Garden, Fenway Park, Museum of Science, New England Aquarium, Boston Harbor Islands, and Museum of Fine Arts.

Register and pay by June 11 and save up to $400! Start making your training and travel plans now; let your colleagues and friends know about SANS Boston 2014. We look forward to seeing you there.

SANS

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

"Learning about security has been very helpful for my job. SEC401 was very informative."
-Linda Runyon, York Risk Service Group

"Please keep up the great work SANS, thanks so much for allowing me to grow professionally."
-Tok Yee Ching, E-cop

"This knowledge is indispensable, utterly necessary, and relevant to every industry."
-Paul Ryan, GDIT

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

Courses-at-a-Glance

		MON 7/28	TUE 7/29	WED 7/30	THU 7/31	FRI 8/1	SAT 8/2
SEC401	**Security Essentials Bootcamp Style**	**Page 1**					
SEC501	**Advanced Security Essentials – Enterprise Defender**	**Page 2**					
SEC504	**Hacker Techniques, Exploits, and Incident Handling**	**Page 3**					
SEC542	**Web App Penetration Testing and Ethical Hacking**	**Page 4**					
SEC560	**Network Penetration Testing and Ethical Hacking**	**Page 5**					
SEC575	**Mobile Device Security and Ethical Hacking**	**Page 6**					
DEV522	**Defending Web Applications Security Essentials**	**Page 7**					
FOR408	**Windows Forensic Analysis**	**Page 8**					
FOR572	**Advanced Network Forensics and Analysis** *NEW!*	**Page 9**					
FOR585	**Advanced Smartphone Forensics** *NEW!*	**Page 10**					
MGT414	**SANS® +S™ Training Program for the CISSP® Cert Exam**	**Page 11**					

@SANSInstitute *Join the conversation: #SANSBoston*

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Jason Fossen
▸ GIAC Cert: GSEC
▸ Masters Program
▸ Cyber Guardian
▸ DoDD 8570

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems.

This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

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

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

> *"SEC401 gives an excellent starting point for securing your networks and devices. You have the opportunity to ask the right questions and understand the answers while interacting with senior security analysts."*
> -Michael Dack, Constellation Energy

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, 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

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 Institute's 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 Cyber Defense Blog.

SECURITY 501

Advanced Security Essentials - Enterprise Defender

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor: Ted Demopoulos
- GIAC Cert: GCED
- Masters Program
- DoDD 8570

Cybersecurity continues to be a critical area for organizations and will increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks will continue to pose a threat to an organization as data become more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

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

"SEC501 is helping me expand my security knowledge by putting the history, and the information in an explanation of real-world technologies."
-Gerald Servidio, General Electric

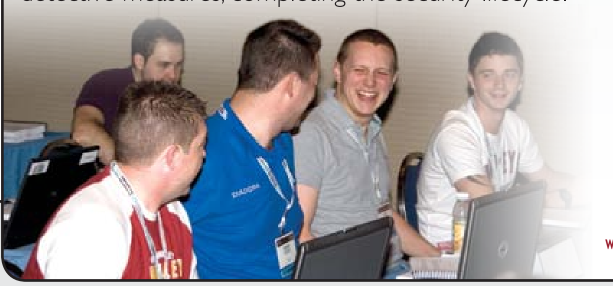
"Very knowledgeable. Top-tier training and industry leading."
-Herbert Monford, Regions Bank

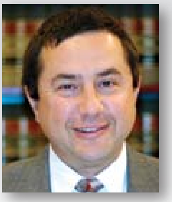
"SEC501 is a great course. Arguably the most informative I have taken in roughly 30 years of working in IT."
-Curt Smith,
Hidalgo Medical Services

www.giac.org

www.sans.edu

www.sans.org/8570





Ted Demopoulos *SANS Certified Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press, and maintains Security Certs, a Web site on Security Certifications. He also has written two books on Social Media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. Ted lives in New Hampshire and more about him is available at Demopoulos Associates. In his spare time, he is also a food and wine geek, enjoys flyfishing, and playing with his children.

SANS
sans.org

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: George Bakos

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

"As a director of IT, SEC504 showed me what my security team should be doing."

-Brian Bounds, Texas Biomedical Research Institute

"The materials in SEC504 directly pertain to my job. Having a better understanding of the techniques used against you help make a better defense. The real-world experiences presented in each session are invaluable for someone with less experience, such as myself. Thanks!"

-Tim Dunaway,
U.S. Army Corps of Engineer

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

George Bakos *SANS Certified Instructor*

George Bakos has been interested in computer security since the early 1980s when he discovered the joys of BBSs and corporate databases. These days he is Technical Director of Intelligence & Response and a Tech Fellow at Northrop Grumman, a global leader in Cybersecurity, Aerospace & Defense. While at the Institute for Security Technology Studies, George was the developer of Tiny Honeypot and the IDABench intrusion analysis system and led the Dartmouth Distributed Honeynet System, fielding deception systems and studying the actions of attackers worldwide. He developed and taught the U.S. Army National Guard's CERT technical curriculum and ran the NGB's Information Operations Training and Development Center research lab for two years, fielding and supporting Computer Emergency Response Teams throughout the United States. A recognized authority in computer security, he has contributed to numerous books and open source software projects; has been interviewed on radio, television, and online publications; briefed the highest levels of government; and has been a member of the SANS Institute teaching faculty since 2001. Outside the lab, George enjoys the beauties of his home state, Vermont, through skiing, ice and rock climbing, and mountain biking.

SANS
sans.org

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, July 28 - Sat, August 2
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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

"SEC542 gives you hands-on experience that other courses do not offer."
-Jon O'Neal, Monster.Com

"Web apps assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."
-James Kelly, Blue Canopy LLP

"I'm a webmaster, not a system admin or an application developer, but the skills learned in SEC542 will help me be aware of potential issues."
-Michael Foster, Troy University

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.

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS
sans.org

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Eric Conrad

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

Who Should Attend

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

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

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

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

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

"I really enjoyed SEC560. As someone who's experienced in penetration testing work, I found the material relevant and learned many new things."
-Carlos Ferreira, Core BTS

"SEC560 provided excellent in-depth use of Metasploit and other security tools."
-Todd Choryan,
Motorola Solutions

"SEC560 provided me with good practice and tools for me to provide to my customers."
-Florent Batard, SCRT

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Eric Conrad *SANS Principal 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.

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

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor:
Christopher Crowley
- GIAC Cert: GMOB
- Masters Program

www.giac.org

www.sans.edu

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 email access as well as 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, 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 practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, 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.

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

"Eye-opening material. I am mesmerized by the course, SEC575. It's time to test apps, they can't be trusted.
-Matthew Britton, BCBSLA

"SEC575 is simply eye opening. Organizations are so busy trying to roll out their BYOD projects without any understanding of the risks. This course is a must for security professionals rolling out BYOD projects."
-Vijay Kora,
Open Solutions Consulting Inc.

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.

DEVELOPER 522

Defending Web Applications Security Essentials

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor:
Johannes Ullrich, Ph.D.

- GIAC Cert: GWEB
- Masters Program

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

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.

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

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.

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
- Application coding errors like SQL Injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

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.

www.giac.org

www.sans.edu

"As the world moves everything online, DEC522 is a necessity."
-Chris Spinder,
B/E Aerospace, Inc.

"Excellent overview of the threat landscape and now I have a much better understanding of how web attacks work."
-Robert Vineyard,
Emory University

Johannes Ullrich, Ph.D. *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 and enjoys blogging about application security.

FORENSICS 408

Windows Forensic Analysis

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Rob Lee

- GIAC Cert: GCFE
- Masters Program

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

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

-Jason Jones, USAF

"FOR408 gave me the framework needed to perform an investigation that is usable for my employer."

-William Lam, SVRCFL

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

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

Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

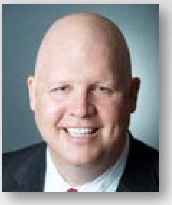
FOR408: Windows Forensic Analysis focuses on the critical digital forensics knowledge of the Microsoft Windows operating system. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations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

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

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

GCFE
www.giac.org

SANS Institute
www.sans.edu



Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington D.C. area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led crime investigations and an incident response team. Over the next 7 years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book "Know Your Enemy, 2nd Edition." Rob is also co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat.

FORENSICS 572

Advanced Network Forensics and Analysis

NEW

SANS
sans.org

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Philip Hagen

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

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

Forensic casework that does not include a network component is a rarity in todays environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way:

BAD GUYS ARE TALKING – WE'LL TEACH YOU TO LISTEN.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Who Should Attend

- Incident response team members
- Law enforcement officers, federal agents, or detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- IT lawyers and paralegals
- Anyone interested in computer network intrusions and investigations

"I research ICS/SCADA environments. I think FOR572 presents a better approach at detecting malware then a traditional approach does."

-Niklas Vilhelm, Norwegian National Security Authority

Philip Hagen *SANS Instructor*

Philip Hagen has over fifteen years of experience in information security, running the gamut from deep technical tasks to management of an entire computer forensic services portfolio. Phil started his security career while attending the US Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer, and was assigned to a base-level year 2000 project management office. The plans he helped create were later used during California's rolling power blackouts. At the Pentagon, he later managed a support team serving 200 analysts. In 2003, Phil shifted to a government contractor, providing technical services for exotic IT security projects. These included systems that demanded 24x7x365 functionality. He supported the design, deployment, and support of a specialized network for 100 security engineers in ten offices. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients. Currently, Phil is the CEO at RedCanary, where he oversees the development and growth of their managed threat detection service, which minimizes the time between a compromise and detection. This helps to support faster and more decisive remediation of network-based intrusions.

FORENSICS 585

Advanced Smartphone Forensics

NEW

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Cindy Murphy

It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individuals movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, or detectives
- IT auditors
- SANS SEC575, FOR563, FOR408, and FOR508 graduates looking to take their skills to the next level

FOR585: Advanced Smartphone Forensics focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. FOR585, originally conceptualized by Eoghan Casey, Heather Mahalik, and Terrance Maguire, addresses todays smartphone technologies and threats by studying real-life investigative scenarios. Dont miss the NEW FOR585!

The hands-on exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones. This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensic professionals. Its time to get smarter!

YOUR TEXTS AND APPS
CAN AND WILL BE USED AGAINST YOU

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

> **"SANS courses have made me want to eat, sleep, and breath security and forensics!"**
> -Cory Flynn, Firewall Experts

> **"If you want to prepare the inevitable considering taking FOR585."**

Cindy Murphy *SANS Instructor*

Detective Cindy Murphy works for the City of Madison, WI Police Department and has been a Law Enforcement Officer since 1985. She is a certified forensic examiner (EnCE, CCFT, DFCP), and has been involved in computer forensics since 1999. She earned her MSc in Forensic Computing and Cyber Crime Investigation through University College, Dublin in 2011. She has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also a part time digital forensics instructor at Madison College, and a part time Mobile Device Forensics instructor for the SANS Institute.

MANAGEMENT 414

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

SANS
sans.org

Six-Day Program
Mon, July 28 - Sat, August 2
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Laptop NOT Needed
Instructor: Dr. Eric Cole
- GIAC Cert: GISP
- DoDD 8570

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

Domain 1: Access Controls
Domain 2: Telecommunications and Network Security
Domain 3: Information Security Governance & Risk Management
Domain 4: Software Development Security
Domain 5: Cryptography
Domain 6: Security Architecture and Design
Domain 7: Security Operations
Domain 8: Business Continuity and Disaster Recovery Planning
Domain 9: Legal, Regulations, Investigations and Compliance
Domain 10: Physical (Environmental) Security

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

Who Should Attend

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of résumé
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Periodic Audit of CPEs to maintain the credential

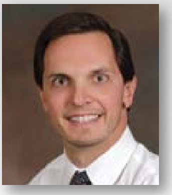
Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

www.giac.org

www.sans.org/8570

Take advantage of SANS CISSP® Get Certified Program currently being offered.
www.sans.org/special/cissp-get-certified-program

> **"The instructor's relationship with their students is key. If a student sees that their instructor cares about their certification attempt, they pay more attention. Eric has done that for me!"**
> -Joseph Cuddy, U.S. Navy



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.

BOSTON 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*

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.

Continuous Ownage: Why you Need Continuous Monitoring

Seth Misenar and Eric Conrad

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

The Bot inside the Machine *Johannes Ullrich, PhD*

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

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

SIFT Workstation - The Art of Incident Response *Rob Lee*

An international team of forensics experts helped create the SANS Investigative Forensic Toolkit (SIFT) Workstation and made it available to the whole community as a public service. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated. Learn how to use the SIFT workstation 3.0, configure, and get up and running finding evil in a variety of forensic cases during this presentation.

Infosec Rock Star: How to be a More Effective Security Professional

Ted Demopoulos

Why are some of us much more effective than others? A very few of us are so effective, and well known, that we might even be called the rock stars of our industry. Now we personally may never be swamped by groupies, but we can learn the skills to be more effective, well respected, and well paid.

Logs, Logs, Every Where – Nor Any Byte to Grok *Phil Hagen*

In this talk, we will discuss one tool that can be very effective in practice: Logstash. Although Logstash is a free and open-source solution intended for system and network administrators to observe live data, it can also provide great value to the forensicator, who must integrate disparate data sources and formats. New developments around Logstash also make it an ideal tool for the system-based forensicator, since supertimeline data can be integrated as well.

SANS 8 Mobile Device Security Steps *Chris Crowley*

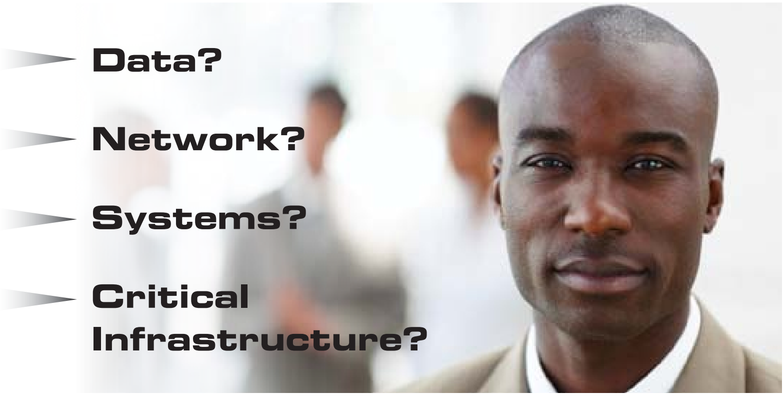
Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided 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.

Vendor Showcase

Wednesday, July 30 | 12:00pm-1:30pm | 5:00pm-7:00pm

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 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

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

Get Certified at
www.giac.org

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

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

SANS Training Courses for DoDD Approved Certifications

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

Compliance/Recertification:

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

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

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

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

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)**

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.

Learn more at

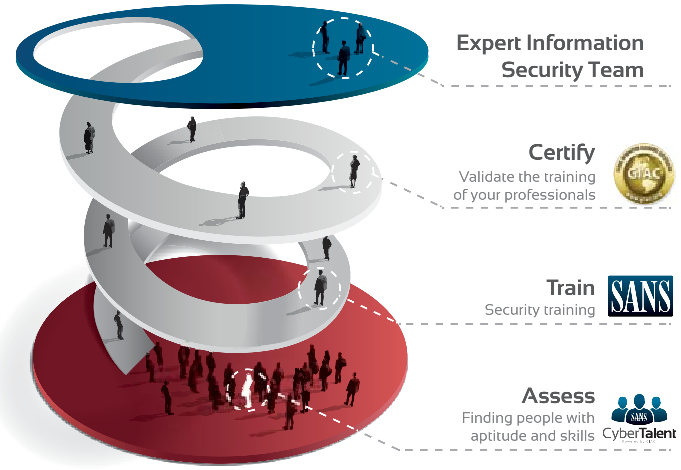
www.sans.edu info@sans.edu

Contact Us to Learn More

www.sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

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



Expert Information Security Team

Certify
Validate the training of your professionals

Train
Security training

Assess
Finding people with aptitude and skills

Benefits of SANS CyberTalent Assessments

For Recruiting

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

For Talent Management

- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps develop a professional development plan

US and Canada 301.654.SANS (7267) EMEA and APAC inquiries: + 44 (0) 20 3598 2363

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

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

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

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

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

ONLINE TRAINING

OnDemand www.sans.org/ondemand
E-learning available anytime, anywhere, at your own pace

vLive www.sans.org/vlive
Online, evening courses with SANS' top instructors

Simulcast www.sans.org/simulcast
Attend a SANS training event without leaving home

OnDemand Bundles www.sans.org/ondemand/bundles
Extend your training with an OnDemand Bundle including four months of e-learning

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of computer based training modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.

SANS SECURING THE HUMAN

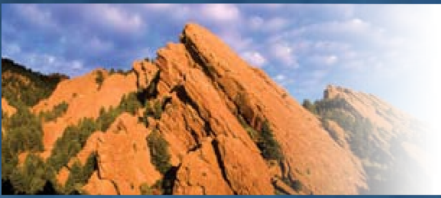
For a free trial visit us at:
www.securingthehuman.org

FUTURE SANS TRAINING EVENTS

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

Digital Forensics & Incident Response SUMMIT

Austin, TX | June 3-10



SANS Rocky Mountain 2014

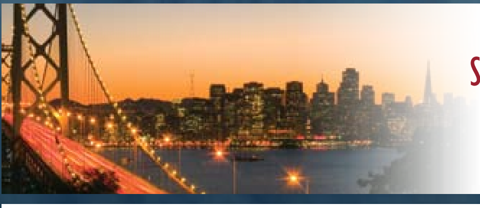
Denver, CO | June 9-14

SANSFIRE 2014

Baltimore, MD | June 21-30

SANS Capital City 2014

Washington, DC | July 7-12



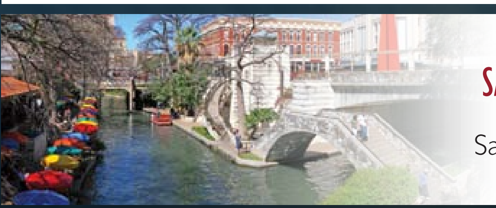
SANS San Francisco 2014

San Francisco, CA | July 14-19

SANS ICS Industrial Control Systems

ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25



SANS San Antonio 2014

San Antonio, TX | August 11-16

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

SANS Chicago 2014

Chicago, IL | August 24-29

SANS BOSTON 2014

Hotel Information

Training Campus
Hilton Boston Back Bay

40 Dalton Street
Boston, MA
www.sans.org/event/boston-2014/location

Special Hotel Rates Available

A special discounted rate of $209.00 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 June 27, 2014. To make reservations please call (800) HILTONS (800-445-8667) or call the hotel directly at (617) 236-1100 and ask for the SANS group rate.

Located in the picturesque neighborhood of Back Bay, the Hilton Boston Back Bay hotel is steps away from everything downtown Boston has to offer. This Back Bay hotel in Boston, Massachusetts is directly across the street from the Hynes Convention Center, only four miles from Boston Logan International Airport, and within walking distance of world-class shopping and dining.

Top 5 reasons to stay at the Hilton Boston Back Bay

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 Boston Back Bay, 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 Boston Back Bay that you won't want to miss!

5 Everything is in one convenient location!

SANS BOSTON 2014

Registration Information

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

Register online at www.sans.org/event/boston-2014/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**6/11/14**	**$400.00**	**6/25/14**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

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

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

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

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 July 9, 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.
www.sans.org/vouchers