THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Boston 2015

Boston, MA August 3-8

Choose from these popular courses:

Continuous Monitoring and Security Operations NEW!

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

SANS Training Program for CISSP® Certification

Advanced Digital Forensics and Incident Response

Advanced Security Essentials – Enterprise Defender

Mobile Device Security and Ethical Hacking

Advanced Smartphone Forensics

Save $400

Register & pay early!

See page 17 for more details.

"SANS courses tend to be enjoyable, and so far I have not encountered a SANS instructor that was not well experienced and entertaining."

-Jonallen Riggins, Blue Canopy Group

Register at sans.org/event/boston-2015

GIAC Approved Training

Please join SANS in **Boston** this summer for our top line-up of cutting-edge cybersecurity training from **August 3-8!** Cyberattacks are the number one national security threat today, and they are increasing in frequency and scale. Security training is your best defense and wisest investment, so come to Boston prepared to hone your skills to defend your critical infrastructure and systems.

At **SANS Boston 2015**, you'll learn useful techniques and tools that you can put to work as soon as you return to your office. Our new **SEC511: Continuous Monitoring and Security Operations** course will show you how to analyze deficiencies, determine and implement security needs, utilize tools, and apply the principles you've learned. SEC511 is one of 10 six-day courses offered in Boston, including courses on security management, incident handling, computer forensics, mobile device security, and web applications security.

SANS courses are taught by accomplished instructors and practitioners in the security industry, including Rob Lee, Paul A. Henry, Johannes Ullrich, Ph.D., Joshua Wright, Eric Conrad, Seth Misenar, Ted Demopoulos, Cindy Murphy, Michael Murr, and Keith Palmgren. SANS instructors apply the concepts and techniques they teach on a daily basis and are considered to be among the best cybersecurity instructors in the world. See inside this brochure for complete instructor bios and course descriptions.

Supplement your SANS training with an **OnDemand Bundle** option when purchasing a course and receive four months of online access to your course's custom e-learning program, including lecture video or audio files, quizzes, and labs – all accessible through your SANS portal account after your live training ends.

SANS Boston 2015 offers several *GIAC* certifications that also align with **DoD Directive 8570**. Complete your training and register for your certification attempt at **www.giac.org**. Also, some of the certifications may be applied toward an accredited Masters of Science degree at **SANS Technology Institute**. To learn more visit **www.sans.edu**.

Our campus for SANS Boston 2015 will be at the **Omni Parker House**, conveniently located along the Freedom Trail and at the foot of Beacon Hill, Boston Common, Quincy Market, and Faneuil Hall. Omni Parker House offers a special discounted rate of $215.00 S/D that will be honored based on space availability. The group rate is currently lower than the government per diem rate. If this changes, the new government per diem rate will be offered. These rates include high-speed Internet in your room and are only available through July 10, 2015. ***Register and pay by June 10 and save $400*** by entering the "**EarlyBird15**" registration discount code.

Let your colleagues and friends know about SANS Boston 2015 and start making your training and travel plans now. Come to Boston to learn from SANS and take in the sights of one of America's most historic cities! We look forward to seeing you there.

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

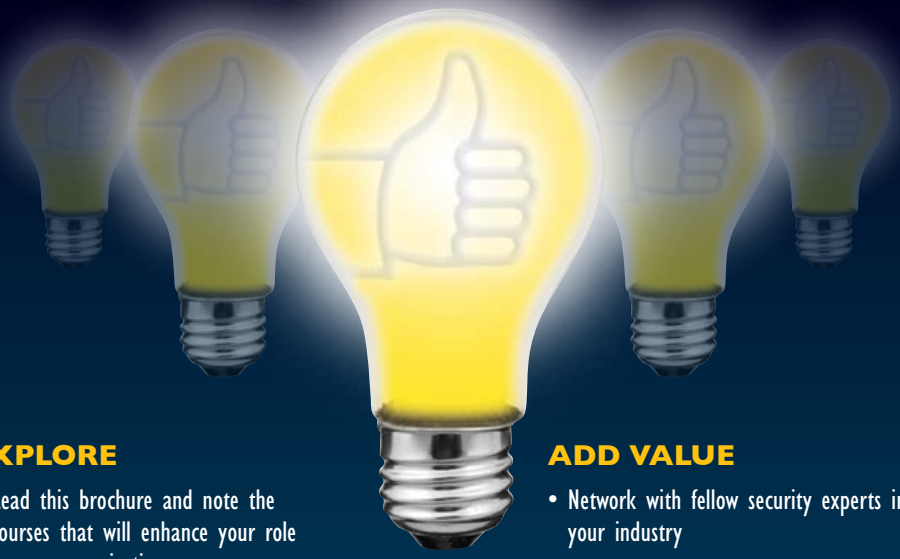
"Not only will you will learn skills, but you will also learn some of the ways your systems are vulnerable. The insight and use of various tools will make my job a lot easier."
-Roland Thomas, U.S. Air Force

"For me the most value is the security perspective of technology, and this course has helped me think about my job differently."
-Afzaal Syed, Ernst & Young

"The whole course will enhance my skillset in order to protect those that can't protect themselves."
-Patrick Barton, PrimeLending

Courses-at-a-Glance

The Value of SANS Training & YOU



EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Ted Demopoulos

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

"This course (SEC401) provides an excellent refresher into the world of computer security, while providing some actionable information that can be used immediately."
-Christopher Deslandes, Dominion Resource Services

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. @TedDemop

SECURITY 501

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Keith Palmgren

- GIAC Cert: GCED
- STI Master's Program
- OnDemand Bundle

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

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

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

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

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

"This course (SEC501) provides a number of valuable tools and techniques to analyze traffic and be able to quickly identify suspicious activity."
-Ken Solomon, NS Corp.

"I learned how to manage the risks, how to protect data, and how to prevent the loss of data that my institution owns."
-Puiu Lucian Chitu, ANCOM

GCED
giac.org

SANS Technology Institute
sans.edu

▶II BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Keith Palmgren *SANS Certified Instructor*

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

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Johannes Ullrich, Ph.D.

- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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

Who Should Attend

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

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

"Awesome course! Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

"I loved this course. I had big expectations, because I have also taken SEC401 Security Essentials course and it was amazing too. All my expectations have been completed."
-Diana Moldovan, Betfair

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

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

giac.org

sans.edu

sans.org/
cyber-guardian


sans.org/8570


BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Johannes Ullrich, Ph.D. *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. 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. His daily podcast summarizes current security news in a concise format. @johullrich

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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

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

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. 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.

"Incident handling is the baseline for cybersecurity, so having a course like SEC504 is great for the beginner and the expert alike. A good solid foundation leads to a great cybersecurity setup." -Robert Fredricks, Parkell Inc.

"This course provides a dual perspective when it comes to threats: offensive and defensive. The mentality of one lends itself to the other. The stress emphasizes this, and demonstrates the need for knowledge." -Michael Jedrey, Commonwealth of Virginia

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

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 @mikemurr

SECURITY 511

Continuous Monitoring and Security Operations

NEW

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar
- OnDemand Bundle

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

"When students walk out, they have a list of action items in hand for making their organization one of the most effective vehicles for frustrating adversaries."
-Eric Conrad and Seth Misenar, SANS

"The material in SEC511 is excellent, and I appreciate the background/pen test material build up to defense. Good defense understands offense."
-Kenneth Hall, BCBSMS

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring (CSM), taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and Day five will greatly increase your understanding and enhance your skills in implementing Continuous Monitoring utilizing NIST framework.

Seth Misenar *SANS Principal Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

SECURITY 542

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

- GIAC Cert: GWAPT
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

Web applications play a vital role in every modern organization. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data.

Who Should Attend

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

Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so, not surprisingly, every major industry study finds that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations.

"The content is very relevant as it features recently discovered vulnerabilities. It also effectively, from my view, caters to various experience levels."
-Malcolm King, Morgan Stanley

"Everything was very well thought out and organized. The URLs used for the labs worked flawlessly. The course content and teaching skills were great!"
-Stephan Hofacker, InfoTrust AG

GWAPT
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

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. @eric_conrad

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Joshua Wright

- GIAC Cert: GMOB
- STI Master's Program
- OnDemand Bundle

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning (ERP) to project management.

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- High probability of the device being hacked, lost or stolen

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 is helping me consolidate my network knowledge in a mobile environment."
-Tony Maurer, DIBP

"I really enjoyed the last android exercise and the iPhone backup analysis, and we applied what was discussed in class."
-Katrina Howard, BAH

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

GMOB
giac.org

SANS Technology Institute
sans.edu

▶II Bundle OnDemand with this course
sans.org/ondemand

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions cyber warriors in the US military, government agencies, and critical infrastructure providers. @joswr1ght

FORENSICS 508

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

- GIAC Cert: GCFA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

DFIR
digital-forensics.sans.org

"The final challenge is excellent and really brought home all the lessons learned."
-Alexandros Papadopoulos, Dell SecureWorks

"This course was incredibly challenging and realistic! The final challenge is intense and really puts you in your place!"
-Reza Salari, DRS Technologies

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occured
- Compromised and affected systems
- What attackers took or changed
- Incident containment and remediation

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved - the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, the incident response course (FOR508) addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

THE ADVANCED PERSISTENT THREAT IS IN YOUR NETWORK – TIME TO GO HUNTING!

Who Should Attend

- Security Operations Center (SOC) personnel and information security practitioners
- System Administrators
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates looking to take their skills to the next level

GCFA
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Rob Lee *SANS Faculty Fellow*
Rob Lee is an entrepreneur and consultant in the Washington, DC 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 seven 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." @robtlee & @sansforensics

FORENSICS 585

Advanced Smartphone Forensics

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Cindy Murphy
- OnDemand Bundle

It is almost impossible today to conduct a digital forensic investigation that does not include a smartphone or mobile device. Smartphones are replacing the need for a personal computer, and almost everyone owns at least one. The smartphone may be the only source of digital evidence tracing an individual's movements and motives, and thus can provide the who, what, when, where, why, and how behind a case. FOR585: Advanced Smartphone Forensics teaches real-life, hands-on skills that help digital forensic examiners, law enforcement officers, and information security professionals handle investigations involving even the most complex smartphones currently available.

Who Should Attend

- Experienced digital forensics examiners
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, or detectives
- IT auditors
- Graduates of SANS SEC575, FOR408, FOR508, or FOR518 who want to take their skills to the next level

digital-forensics.sans.org

"Cindy is brilliant!"
-Michal Sadlon,
NATEO CCD CoE

"It's real-world practical information and not just textbook!"
-Reza Salari,
DRS Technologies

"Cindy is awesome! She fully understands what is happening in the field and how we can do our job better."
-John Peck, Shell Oil

The course focuses on smartphones as sources of evidence, providing students with the skills needed to handle mobile devices in a forensically sound manner, manipulate locked devices, 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. Students will walk away with knowledge they can immediately put to use on their next smartphone investigation.

FOR585: Advanced Smartphone Forensics you will learn:

- **Smartphone Capabilities:** Determine the who, what, when, where, why, and how of a case. Who used a smartphone? What did the user do on a smartphone? Where was the smartphone located at key times? What online activities did the user conduct using a smartphone, and when?
- **How to Recover Deleted Data:** Use manual decoding techniques to recover deleted data stored on smartphones and mobile devices.
- **How to Detect Data Stored in Third-Party Applications:** Who did the user communicate with using a smartphone and why are these activities sometimes hidden?
- **How to Detect Malware:** Detect smartphones compromised by malware using forensics methods.
- **How to Bypass Locks:** Bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes.

▶II **Bundle OnDemand** with this course
sans.org/ondemand

Cindy Murphy *SANS Certified 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. @cindymurph

MANAGEMENT 414

SANS Training Program for CISSP® Certification

Content Updated for New Exam! Effective April 15th

SANS

Six-Day Program
Mon, Aug 3 - Sat, Aug 8
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Paul A. Henry

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

Need training for the CISSP® exam?

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand 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® 8 domains
- Security professionals and managers looking for practical ways to apply the 8 domains of knowledge to their current activities

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

Students Will Learn:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

giac.org

sans.org/8570

"I think Paul is an awesome instructor and his knowledge, experience, and energy really make the classes enjoyable."
-Jim Shields, Tiff Advisory Services

"As a developing security professional, this course sufficiently covers the core concepts needed to obtain CISSP."
-Kurt Zimmerman, Protivity Inc.

Bundle OnDemand with this course
sans.org/ondemand

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

Paul A. Henry *SANS Senior Instructor*

Paul Henry is a Senior Instructor with the SANS Institute and one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

KEYNOTE: The SANS360 *Led by Rob Lee*

In one hour, 8-10 security experts will discuss the latest security trends and techniques that will make a difference in the way you approach security. Topics will include hacking, forensics, penetration testing, security operations, and continuous monitoring. If you have never been to a lightning talk it is an eye-opening experience. Each speaker has 360 seconds (6 minutes) to deliver their message. This format allows SANS to present 8-10 experts within one hour, instead of the standard one presenter per hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just 6 minutes away.

iOS Game Hacking: How I Ruled the Worl^Hd and Built Skills For AWESOME Mobile App Pen Tests *Josh Wright*

I am a terrible video game player. I lack the skills to competitively arrange words with colleagues, crush jelly beans, or achieve a high score arranging numbers by threes. However, what I lack in video game competition, I make up for in iOS app hacking. In this talk, we'll explore the profitable market of iOS games, looking at several techniques that are used to cheat, hack, or even steal from iOS game developers. You'll be able to apply these techniques to give yourself a leg up on your next gaming experience. Most importantly, each and every technique we'll discuss is also directly applicable to penetration testing and assessing the security of the iOS apps your organization uses each and every day. Learn to pwn games while becoming a better app pen tester! What's not to like?

Instant Expert: Legitimately and Ethically *Ted Demopoulos*

Part of the Infosec Rock Star Series of talks: We naturally build expertise with experience, but we don't necessarily build "Expert Status". There are many reasons to develop expert status:

- Expert status gives you more influence
- People listen to experts readily
- Experts can make a bigger and more positive impact
- Experts are well paid
- Experts have a lot of flexibility to follow their passions in life

Even the mere concept of what constitutes an expert confuses most people. An expert is "a person with extensive knowledge or ability" which means they know significantly more than others. It is a relative term however. It doesn't mean #1 Expert in the world. It doesn't mean there is nothing else left to learn. Chances are that you are already an expert on several topics. In this talk we examine exactly what an expert is (again, you probably already are an expert), and the multiple ways to quickly, legitimately, and yes, sometimes even nearly instantly, develop expert status.

The 14 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified 14 absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the fourteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

The Internet of Evil Things *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. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. 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).

Continuous Monitoring and Real-World Analysis *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. Modern threats require a paradigm shift in the way we perform analysis and monitoring. This talk will help you face the problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

DFIR Advanced Smartphone Forensics *Cindy Murphy*

Forensic investigations often rely on data extracted from smartphones and tablets. Smartphones are the most personal computing device associated to any user and can therefore provide the most relevant data per gigabyte examined. Commercial tools often miss digital evidence on smartphones and associated applications, and improper handling can render the data useless. We have created a poster as a cheat sheet to help you remember how to handle smartphones, where to obtain actionable intelligence, and how to recover and analyze data on the latest smartphones and tablets. This presentation provides an overview of useful data that can be extracted from mobile devices and we will walk through the new Smartphone Forensics Poster.

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.

"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 **giac.org**

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $629 when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- Labs
- MP3s and Videos of lectures
- Subject-Matter Expert support

Visit sans.org/ondemand/bundles for more information about OnDemand Bundles now.

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Healthcare - Phishing

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

SANS SECURING THE HUMAN

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

SANS Technology Institute

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive, rigorous, graduate education experience.

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.

POST★9/11 GI BILL

Now eligible for Veterans Education benefits!
Earn industry-recognized GIAC certifications throughout the program
Learn more at www.sans.edu | info@sans.edu

GIAC

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).
More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

FUTURE SANS TRAINING EVENTS

SANS/NH-ISAC Healthcare Cybersecurity SUMMIT & TRAINING
Atlanta, GA | May 12-19

SANS Pen Test Austin 2015
Austin, TX | May 18-23 | #PenTestAustin

SANS Houston ICS Security Training
Houston, TX | June 1-5 | #SANSICS

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS Rocky Mountain 2015
Denver, CO | June 22-27 | #SANSRockyMtn

SANS Capital City 2015
Washington, DC | July 6-11 | #SANSDC

SANS Digital Forensics & Incident Response SUMMIT & TRAINING
Austin, TX | July 7-14 | #DFIRSummit

SANS San Jose 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS Minneapolis 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS Cyber Defense SUMMIT & TRAINING
Nashville, TN | August 11-18 | #CyberDefenseSummit

SANS San Antonio 2015
San Antonio, TX | August 17-22 | #SANSSATX

SANS Security Awareness SUMMIT & TRAINING
Philadelphia, PA | August 17-25 | #SecAwareSummit

SANS Virginia Beach 2015
Virginia Beach, VA | August 24 - Sept 4 | #SANSVaBeach

SANS Chicago 2015
Chicago, IL | August 30 - September 4 | #SANSChicago

SANS Crystal City 2015
Crystal City, VA | September 8-13 | #SANSCrystalCity

SANS Network Security 2015
Las Vegas, NV | September 12-21 | #SANSNetworkSecurity

SANS Baltimore 2015
Baltimore, MD | September 21-26 | #SANSBaltimore

SANS Seattle 2015
Seattle, WA | October 5-10 | #SANSSeattle

SANS Tysons Corner 2015
Tysons Corner, VA | October 12-17 | #SANSTysonsCorner

SANS Cyber Defense San Diego 2015
San Diego, CA | October 19-24 | #SANSCyberDefSD

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events 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 sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training sans.org/private-training
Live Onsite Training at Your Office Location. Both in Person and Online Options Available

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

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

ONLINE TRAINING

OnDemand sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive sans.org/vlive
Online, Evening Courses with SANS' Top Instructors

Simulcast sans.org/simulcast
Attend a SANS Training Event without Leaving Home

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

Do You Enjoy Live Classrooms But Can't Always Travel?

SANS offers live ONLINE TRAINING in both day and evening formats.

vLive

Six weeks of evening classroom sessions via GoToTraining software, with six months of online access to course materials, quizzes, and labs.

Simulcast

One week of daytime classrooms via GoToTraining software, with four months of online access to course materials, quizzes, and labs.

Both formats also include all printed course materials and Subject-Matter Expert support.

To see a list of upcoming courses in either format, visit:

sans.org/vlive *or* **sans.org/simulcast**

SANS BOSTON 2015

Hotel Information

Training Campus
Omni Parker House

60 School Street
Boston, MA 02108
sans.org/event/boston-2015/location

2015 marks the 160th anniversary of this legendary hotel's history. Old-world charm and elegance are accompanied by all of the modern conveniences of a world-class establishment. Nestled in the heart of downtown Boston, Omni Parker House is located along the Freedom Trail and at the foot of Beacon Hill, Boston Common, Quincy Market and Faneuil Hall marketplace.

Special Hotel Rates Available

A special discounted rate of $215.00 S/D will be honored based on space availability.

At this time, the group rate is currently lower than the government per diem rate. If this changes, the new government per diem rate will be offered. These rates include high-speed Internet in your room and are only available through July 10, 2015.

Top 5 reasons to stay at Omni Parker House

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 Omni Parker House, 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 Omni Parker House that you won't want to miss!
5. Everything is in one convenient location!

SANS BOSTON 2015

Registration Information

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

Register online at sans.org/event/boston-2015/courses

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

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

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**6/10/15**	**$400.00**	**7/1/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

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 15, 2015 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers


Open a
SANS
Account
Sign up for a
SANS Account
and receive free
webcasts, newsletters,
the latest news and
updates, and many other
free resources.
sans.org/account