THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS Boston 2016

August 1-6

SANS OFFERS HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Protect your company
and advance your career with
information security training from SANS!

Ten courses on

CYBER DEFENSE

PEN TESTING

DIGITAL FORENSICS

SECURITY MANAGEMENT

"SANS always offers real-world applicable training, I can take what I learned today and apply it when I return to work."

-Mark Burns, LG&E KU Energy

REGISTER AT

sans.org/boston

GIAC-Approved Training

SAVE $400

by registering and paying early!

See page 17 for more details.

Cyber attacks 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, and **SANS Boston 2016** from August 1-6 will provide you with the best information and software security training anywhere.

You will learn useful techniques and tools that you can put to work as soon as you return to your office. SANS courses are taught by accomplished instructors and practitioners in the security industry, including Rob Lee, Paul A. Henry, Johannes Ullrich, Eric Conrad, Seth Misenar, Joshua Wright, Michael Murr, Ted Demopoulos, Ryan Johnson, and me, Stephen Northcutt. SANS instructors teach and apply real-world concepts and techniques on a daily basis and are considered to be among the best cybersecurity instructors in the world.

Nine of our information security courses will prepare you for a prestigious GIAC certification in just one week of study. You can also supplement your training with an OnDemand Bundle providing you four months of online access to our OnDemand e-learning platform. And your live, hands-on SANS training experience also counts as progress towards a Graduate Certificate or Master's Degree in Information Security Management or Engineering via the SANS Technology Institute.

Review course descriptions, instructor biographies, evening talks, keynote speakers, and hotel information inside this catalog to learn what you will gain from attending SANS Boston 2016. **Register and pay before June 8 to receive the early-bird discount.**

We hope that you attend, because SANS knows that you – our students – are securing the world from cybercrime. We are recognized worldwide as the leading organization for training professionals in cybersecurity, and we want to use our expertise to help you succeed. Prepare to hone your skills to defend your critical infrastructure and systems!

If I can answer any questions about SANS Boston or help you choose the appropriate course please reach out to me at **stephen@sans.edu**. I hope you join us and take in the sights of one of America's most historic cities. I look forward to seeing you there.

Stephen Northcutt
SANS Boston 2016 Chair

Stephen Northcutt

Below is what attendees have said about their SANS training experience:

"This course will change the way you look at the environment you work in, and you will never be the same."
-Shaun Gatherum, NuScale Power

"This training introduced me to an aspect of IT interface that I was unfamiliar with and I now have a better understanding of the business side."
-Dallas Haselhorst, Sicoir Computer Technologies

"This training is valuable because it helped me to understand network security from various types of prevention."
-Stephen L Perry, Ardent Health Services

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 the SANS Voucher Program 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!

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 1 - Sat, Aug 6
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Paul A. Henry

giac.org

sans.edu

sans.org/8140

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"Paul Henry is an excellent instructor who presents large volumes of information effectively."
-ROWLEY MOLINA, ALTRIA

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.

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*!

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
- 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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the rise of advanced persistent threats, 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.

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. 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 U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert in perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. @phenrycissp

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Aug 1 - Sat, Aug 6
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, PhD

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 analysts (all levels)
- Network engineers
- System, security, and network 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 will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

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

"SEC503 directly covers the necessary knowledge and skill set I use every day at my job. The added insight is worth the price."
-Michael Garrett, Federal Reserve Bank of San Francisco

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/8140

Bundle OnDemand
with this course
sans.org/ondemand

"I enjoyed the deeper technical content, getting hands-on experience with the course content packets, and the real-world examples Dr. Ulrich presented in this course."
-Ben Roe,
Koch Business Solutions

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. In 2000, he founded DShield.org, 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 joining 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 based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"SEC504 is practical and can be utilized immediately."
-Abraham Rivera, Morgan Stanley

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
- 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

"I love Mike Murr's analogies they are spot on and help break down complex information. The intensity of the course is matched by the knowledge and enthusiasm of the instructor." -Elizabeth Murrell, Boston Medical Center

This course helps you turn the tables on computer attackers by helping you understand their 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. 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 for, 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. This 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.

"This course is foundational and core strength building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both adversary and defender." -Araceli Ari Gomes, Dell Secureworks

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and 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). He has also 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. He 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

SEC511:
Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

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

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"Seth's experience and expertise in the subject domain are especially useful for me to understand customer requirements and, thereafter, deploy an appropriate monitoring environment."
-Ryan Wong,
Accel Systems & Techlologies

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat 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
- Security Operations Center analysts, engineers, and managers
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)
- Computer Network Defense analysts

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.

"This training is valuable because it helped me to understand network security from various types of prevention and provided good insight into endpoint security."
-Stephen L. Perry, Ardent Health Services

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 is 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 this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

Seth Misenar *SANS Senior Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security thought 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 and the Health Insurance Portability and Accountability Act, and as 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 that include CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

SEC542:

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Aug 1 - Sat, Aug 6
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"Eric is an excellent instructor! He always has excellent real-world examples to back up instruction."
-ERNIE H. U.S. NAVY

Web applications play a vital role in every modern organization. However, if your organization doesn't properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Who Should Attend

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

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

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 business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find 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 effective web application penetration testing requires something deeper.

SEC542 enables students to 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. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

Eric Conrad *SANS Senior 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 healthcare. 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 ericconrad.com. @eric_conrad

SEC575:
Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Mon, Aug 1 - Sat, Aug 6
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

giac.org

sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"Taking this course was a great opportunity to ask an expert all my questions, good broad overview and mobile threats background!"
-Tom G., GovCert UK

"I appreciate Joshua's effort to help all students regardless of the issue."
-David E., DoD

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports a wide range of wireless technologies all ripe for attack. There's no need to imagine any further because you actually already have this today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

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

NOW COVERING ANDROID MARSHMALLOW, iOS 9, APPLE WATCH AND ANDROID WEAR

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

LEARN HOW TO PEN TEST THE BIGGEST ATTACK SURFACE IN YOUR ENTIRE ORGANIZATION

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as having prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

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 for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joshwr1ght

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, Aug 1 - Sat, Aug 6
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

giac.org

sans.edu

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

DFIR
digital-forensics.sans.org

"Rob is great and very knowledgeable! He balances complexity with easy to understand examples."
-Andy Hoff, Medtronic

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber crime occurring on its computer systems and within its networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

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 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

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

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 vulnerability discovery and exploit development teams, 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

FOR572:
Advanced Network Forensics and Analysis

SANS

Six-Day Program
Mon, Aug 1 - Sat, Aug 6
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ryan Johnson

giac.org

sans.edu

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

DFIR
digital-forensics.sans.org

"The labs – practice towards excellence – and the instructor's real-world stories provide valuable experiences and insight."
-Nate Dewitt, eBay, Inc.

Forensic casework that does not include a network component is a rarity in today's 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.

Who Should Attend

- Incident response team members and forensicators
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

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.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cyber crime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

Ryan Johnson *SANS Instructor*

Ryan is a Senior Director and lead incident responder in the Cyber Division of the consulting firm Alvarez & Marsal. He was a co-owner of Forward Discovery, where he was the lead incident responder and supported the maintenance of the Raptor acquisition tool. Ryan has been investigating crimes in the digital realm for more than 10 years, including performing media exploitation for the U.S. Army in Iraq. He has run multiple large-scale breach investigations and also provides clients with proactive assessments to help them identify security gaps and already-compromised systems. Ryan teaches with the U.S. State Department's Anti-Terrorism Assistance Program and is a co-author of several of its digital forensics courses. Ryan co-authored *Mastering Windows Network Forensics and Investigations, Second Edition*. His industry credentials include the GNFA, GCIH, CFCE, DFCP, EnCE, and PCIP certifications. He earned an M.S. from Dalhousie University and a B.S. from Queen's University. @ForensicRJ

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Aug 1 - Fri, Aug 5
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: Stephen Northcutt

giac.org

sans.edu

sans.org/8140

Bundle OnDemand
with this course
sans.org/ondemand

"Awesome content and delivery! Mr. Northcutt's excitement for security is contagious."
-Shannon B.,
311th Signal Command

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

Who Should Attend

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

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

Knowledge Compression™

Maximize your learning potential!

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

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and served as the founding president of the SANS Technology Institute, an accredited graduate school focused on cybersecurity. Stephen is author/coauthor of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security 2nd Edition*, *IT Ethics Handbook*, and *Network Intrusion Detection 3rd Edition*. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings. He leads the Management 512 Alumni Forum, where hundreds of security managers post questions. He is the lead author for MGT512, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570. He also is the lead author/instructor for MGT514. Stephen blogs at the SANS Security Laboratory and is on the NewsBites and SANS Analyst teams. He has been involved in a number of security startups including SourceFire, Tenable, Savant Protection and Zimperium, and currently serves as director of academic advising for SANS.EDU. @StephenNorthcut

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, Aug 1 - Fri, Aug 5
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Ted Demopoulos

SANS Technology Institute
sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This is a great foundational course as we realize the importance of bringing a business perspective to security." -Nairobi Kim, Wells Fargo

"Ted was amazing and absolutely great, and the best trainer I've had so far." -Angel Camacho Badajoz, Roche & Genentech

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team-lead or management responsibilities

Develop Strategic Plans

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

Create Effective Information Security Policy

Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that?" Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

Develop Management and Leadership Skills

Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

"This training was valuable because it helped me examine myself from an outside point of view." -DJ, Zoetis

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 ongoing 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. 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. In his spare time, he is also a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

Evening talks 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: **Writing Tech: Career Advancement and You**

– Joshua Wright

Tech writing is a great way to differentiate you from your peers, opening up opportunities for career advancement and peer approbation. You also get to look really smart when you use words like "approbation." In the last decade, Josh has learned a thing or two about tech writing as the author or co-author of four books and six SANS courses. Things like struggling to get the words out. Things like getting checks from your publisher that are smaller than the price of mailing them. Things like Hofstadter's law ("It always takes longer than you expect..."), working with co-authors, and the extreme hypochondria variety known only to writers. Come to this talk to learn about tech writing, and the opportunities it opens up for your career. Come to learn about the techniques that can make tech writing successful for you. Come to hear the funny, sad, and outrageous stories that only come from a decade of tech writing. Come to this talk and leave with a sense of purpose, inspiration to grow your career, and peer approbation.

PANEL: **My Browser is Not My Friend**

– Moderator: Stephen Northcutt; Panelists: Eric Conrad, Ted Demopoulos & Seth Misenar

One of the security researchers I follow is Richard Bejtlich, so when I saw he did a review of the book *Web Application Obfuscation*, I read it. What he wrote blew my mind: "After finishing WAO, it's only appropriate to say 'wow.' In short, I had no idea that web browsers (often called 'user agents' in WAO) are so universally broken." I started looking into this and I have to say he is correct. I tried some of the simple obfuscations and in some cases Edge, Chrome, Firefox, Safari and Opera all responded differently. This does not bode well for organizations running more than one browser. And that is the tip of the iceberg. This panel will discuss some of the problems, good practice, and promising solutions.

The Security Impact of IPv6 *– Johannes Ullrich, Ph.D.*

IPv6 is more than just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the "DC" to "AC" power conversion in the late 1890s. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocol's opportunities are not well understood, and if IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody's pet.

Investing for Retirement *– Stephen Northcutt*

When I turned 50 I joined AARP so I could get 20% off Regal Theaters popcorn and other swell discounts, but it seemed that every issue of the association's magazine had an article on people not saving enough to retire. Having said that, saving for retirement sometimes seems silly: the best interest rate I have seen on a savings account is 0.7% and that is probably less than the cost-of-living increases. If any of us are going to retire, we will need to invest and invest wisely. Since I am older than most SANS instructors, it occurred to me that I could be one of the first to face the retirement issue. For the past five years, I have been looking at the options to generate enough monthly income to retire on and have found the results rather surprising. This talk summarizes my research. It will cover many of the financial vehicles that are available, and for each one we'll cover the pitch, the catch, and my best assessment of how to use (or avoid) that vehicle. The talk is meant to encourage members of the audience to begin thinking about their financial portfolio and retirement options. Best of all, I promise I will not try to sell anybody anything.

Beware the Reaper – *Ryan Johnson*

200+ days. That's how long the average attacker is in an environment undetected. That's when either the FBI calls to say, "You have a problem," or Brian Krebs calls for a comment to his soon-to-be-released blog post about your company. Nobody wants that. So, if the attackers are there, how do we find them? It's not a needle in a haystack, it's a needle in a stack of needles! If you or your client don't have the budget to store a year's worth of logs or six months worth of packet captures, or you don't have the new million dollar widget in place, where do you start? In this talk, we will discuss a proven approach that can help answer the question, "Are we owned?" You will see how to look across the entire enterprise and get a snapshot assessment of the compromise status of the environment. You can do this by using nothing more than the lethal forensicator knowledge you already possess (and maybe a big magnet). You'll quickly see how you can narrow down the massive dataset to something more manageable – allowing you to get to the important answer faster.

Evolving Threats – *Paul A. Henry*

For nearly two decades defenders have fallen into the "crowd mentality trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and on attempting to outwit an attacker's delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years. This presentation will highlight recent and breaking developments in the evolution of both attacks and defenses.

Welcome Threat Hunters, Phishermen, and Other Liars – *Rob Lee*

Over the past few years, a new term has continually popped up in the IT Security community called "threat hunting." While the term seems like it is new, it really is the reason all of us joined IT security in the first place: to find evil. While I was at Mandiant and in the U.S. Air Force, "finding evil" was in fact our tagline when we were on assignments.

This talk was put together to outline what exactly "threat hunting" means and step you through how it works. When I first started in IT Security back in the late 1990s, my job was to find threats in the network. This led to automated defenses such as Intrusion Detection Systems, monitoring egress points, logging technology, and monitoring the defensive perimeter hoping nothing would get in. Today, while the community is trying to identify intrusions, threat hunting has evolved to be something a bit more than the loose definition of "finding evil," primarily due to the massive amount of incident response data currently collected about our attackers. This data has evolved into cyber threat intelligence.

The hunt to "find evil" will be better targeted if you're armed with cyber threat intelligence about what you're looking for and what your adversaries are likely interested in. Such intelligence can be used to great effect when employed properly and proactively against a threat group. Threat hunting has improved the accuracy of threat detection because we can now focus our searching on the adversaries exploiting our networks – humans hunting humans. Even with knowing where to look, tools are now being introduced to help make hunting more practical across an enterprise.

VENDOR EVENT

The IPM Chowder Event

The Boston faculty team consulted with the GIAC Advisory Board and determined that one of the crucial problems to solve is better Identity (and just as important) Privilege Management. The team then completed an industry survey to determine the leading vendors and designed an evening event to present the information in a "PowerPoint Lite" format. Each vendor will present the key points of their product. The vendors have been invited to have a customer who uses the product speak as well. We will also be serving variations of chowder and an adult beverage. You vote on which chowder, speaker, and product is most compelling!

How Are You Protecting Your

- Data?
- Network?
- Systems?
- Critical Infrastructure?

"I'm Trey Blalock, GWAPT, GCFA, GPEN, and a member of the GIAC Advisory Board. My certifications have helped open doors for me in my cybersecurity career. The security of your cyber assets depends on the skills and knowledge of your security team!"

Get GIAC Certified!

GIAC offers over 30 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

GWAPT GCFA GPEN GIAC

Follow us on Twitter **@CertifyGIAC**

Get Certified at **giac.org**

ONLINE Training Options

FOR SANS BOSTON 2016

OnDemand Bundle

Extend your SANS Boston 2016 course online after the event, with:

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

Learn more about your Online Training options at **sans.org/online** or contact us via **ondemand@sans.org**.

FUTURE SANS TRAINING EVENTS

Security Operations Center
SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

SANSFIRE 2016
Washington, DC | Jun 11-18

Digital Forensics & Incident Response
SUMMIT & TRAINING 2016
Austin, TX | Jun 23-30

Salt Lake City 2016
Salt Lake City, UT | Jun 27 - Jul 2

Rocky Mountain 2016
Denver, CO | Jul 11-16

Minneapolis 2016
Minneapolis, MN | Jul 18-23

San Antonio 2016
San Antonio, TX | Jul 18-23

ICS Security & Training – Houston 2016
Houston, TX | Jul 25-30

San Jose 2016
San Jose, CA | Jul 25-30

Security Awareness
SUMMIT & TRAINING 2016
San Francisco, CA | Aug 1-10

Portland 2016
Portland, OR | Aug 8-13

Dallas 2016
Dallas, TX | Aug 8-13

Chicago 2016
Chicago, IL | Aug 22-27

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

SANS BOSTON 2016

Hotel Information

Training Campus
Omni Parker House

60 School Street
Boston, MA 02108
sans.org/event/boston-2016/location

This grand luxury hotel has been symbolic of Boston's rich history and culture since 1855. 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 lower than the government per diem rate. If this changes, the new government per diem rate will be offered with proper ID. These rates include high-speed Internet in your room and are only available through 5pm EST on July 8, 2016.

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 2016

Registration Information

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

Register online at sans.org/boston

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 **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**6-8-16**	**$400.00**	**7-6-16**	**$200.00**

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

sans.org/vouchers

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 13, 2016 – processing fees may apply.

Open a **SANS Portal Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

sans.org/security-resources