THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Seattle 2015

Seattle, WA October 5-10

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Advanced Digital Forensics and Incident Response

Securing Windows with PowerShell and the Critical Security Controls

Advanced Security Essentials – Enterprise Defender

Mobile Device Security and Ethical Hacking

"You can't go wrong with taking a SANS course. Receiving updated or current training along with the tools that will help you to get your work done more efficiently."

-David Fava, The Boeing Company

GIAC Approved Training

Register at sans.org/event/seattle-2015

SAVE **$400** by registering & paying early!

See page 13 for more details.

SANS Seattle 2015 from **October 5-10** has an exciting lineup of hands-on training courses in IT security, forensics, and mobile device security. Protecting your data is more critical than ever, and when it comes to cybersecurity the best defense is a strong offense. So join us at SANS Seattle 2015 for the most up-to-date security training available to thwart malicious cyber threats against your organization's devices and systems.

The SANS Seattle 2015 brochure highlights each of the courses offered as well as our stellar line-up of instructors, including Jason Fossen, Dave Shackleford, Bryce Galbraith, Christopher Crowley, Bryan Simon, and Jake Williams. SANS instructors are experienced industry practitioners who will impart their expert guidance and provide the skills you need to prevent or mitigate cyber attacks against your organization as soon as you get back to your office.

All courses at SANS Seattle 2015 offer ***GIAC certification*** to complement your training. Professionals who are GIAC certified are recognized as experts in the IT industry and are sought after by government, military, and industry. See **www.giac.org** for details.

Corporations are in need of security professionals who are both technically advanced and have effective communications and management skills. ***SANS Technology Institute*** offers two different cybersecurity master's degrees as well as post-baccalaureate graduate certificates in specialized fields such as penetration testing and ethical hacking, incident response, and cybersecurity engineering. To learn more see **www.sans.edu**.

You can supplement your training at SANS Seattle 2015 with the ***SANS OnDemand Online Bundle***, which provides you with four months of online access to our e-learning platform. The bundle is available for the course you purchase on your SANS training registration. Details for this option are explained at **www.sans.org/ondemand/bundles**.

Our campus for SANS Seattle 2015 is the **Renaissance Seattle Hotel** in the heart of downtown. The hotel features stunning views of Puget Sound, the mountains, and the city skyline. You can combine your cybersecurity training with a tour of Seattle's Pike Place Market, the oldest continuously operating market in the United States. Or you can explore the grandeur of the Pacific Northwest with outdoor day trips to Mount Rainier, Bainbridge Island, San Juan Islands, Snoqualmie Falls, or the Mount St. Helens National Volcanic Monument.

A special discounted rate of $179.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through September 4, 2015. Also, you can **save $400** when you pay for any SANS Seattle course by **August 12**.

Let your colleagues and friends know about SANS Seattle 2015 and start making your training and travel plans now. We look forward to seeing you in Seattle!

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

"The instructor made the material very entertaining, and presented the information in a way that flowed – excellent!"
-Joshua Leak, BB&T

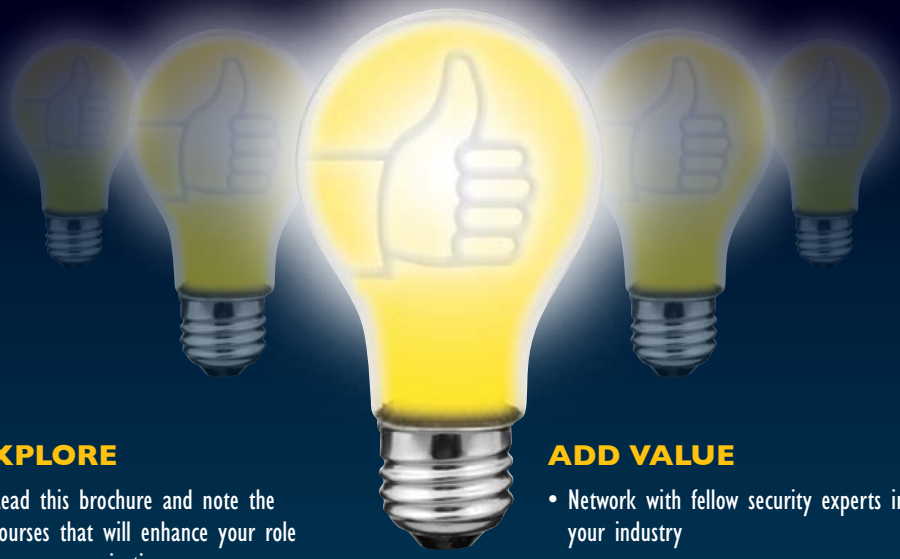
"Excellent tips and links provided today – far more than I was anticipating and there are many that I plan to use."
-Paul Puskorius, The College Board

"After years of imaging and analysis, I learned more in one day then six months in this field."
-Don Malone, Beyond Inc.

"Lots of information that was useful and directly applicable."
-Joseph Weber, Regions Financial

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, Oct 5 - Sat, Oct 10
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryce Galbraith

- 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

"Great explanations on crypto! Took a semester long course and this was much better. The instructor maintains the energy for the entire class and never hesitates to answer questions."
-David Lawrence, Livermore National Laboratory

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he holds several security certifications and speaks at conferences around the world. @brycegalbraith

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Oct 5 - Sat, Oct 10
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Bryan Simon

- 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

"This training is valuable to my company because it allows me to learn about aspects of security I don't normally get exposed to on a normal basis.
-Brendon Rager, Talquin Electric Cooperative

"This course is fun and fast paced! I'm really enjoying the class, plus the time is going by so fast! Great information and tools."
-Danielle Perchert, Sandia National Labs

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.

GCED
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in I.T. Security, and was most recently profiled by McAfee (part of Intel Security) as an I.T. Hero. Bryan holds 11 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Oct 5 - Sat, Oct 10
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Dave Shackleford

- 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

"This course gave me a better understanding of what a hacker can do and how he does it – which will help me with incident handling."
-Jill Gallagher, HSBC

"This course helped me fill in the finer details and gaps in my knowledge. I understood the higher level concepts. I have worked with a few of the tools but this helped put it all together."
-Jenna Esparza, Los Alamos National Laboratory

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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand with this course
sans.org/ondemand

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book *Virtualization Security: Protecting Virtualized Environments*, as well as the coauthor of *Hands-On Information Security* from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. @daveshackleford

SECURITY 505

Securing Windows with PowerShell and the Critical Security Controls

Six-Day Program
Mon, Oct 5 - Sat, Oct 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

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

How can we defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that lead to advanced persistent threat malware infections? We tackle these tough problems in **SEC505: Securing Windows with PowerShell and the Critical Security Controls**.

Who Should Attend

- Anyone who wants to learn PowerShell
- Windows security engineers and system administrators
- Anyone implementing the Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- Anyone who needs to reduce APT malware infections

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defenses against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is useful, but there is no simple patch against their abuse. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future. This requires more than just reactive patch management - we need to proactively design security into our systems and networks. That is what SEC505 is about.

"SEC505 course content is excellent. In-class activities were very valuable. Very good teaching skills and knowledge."
-Jesus Perez, Texas A&M University

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows administrators, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills, so knowing PowerShell is a great way to make your résumé stand out. This course devotes the entire first day to PowerShell, then we do more PowerShell exercises throughout the rest of the week. Don't worry, you don't need any prior scripting experience to attend.

"I have been to other windows training, but never one with a focus on security – this has been an eye-opening experience. I hope to attend more events like this in the future."
-Dewayne Wasson, Kellogg Company

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) exam to certify your Windows security expertise. The GCWN certification counts toward getting a Master's Degree in information security from the SANS Technology Institute (**sans.edu**) and also satisfies the Department of Defense 8570 computing environment requirement.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security!

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

Jason Fossen *SANS Faculty Fellow*

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

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Mon, Oct 5 - Sat, Oct 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Christopher Crowley

- 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
- The high probability of device loss or theft, and more

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

SEC575: Mobile Device Security and Ethical Hacking is designed to help organizations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course will help you build the critical skills to support your organization's secure deployment and use of mobile phones and tablets. You will learn how to capture and evaluate mobile device network activity, disassemble and analyze mobile code, recognize weaknesses in common mobile applications, and conduct full-scale mobile penetration tests.

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"Chris is an awesome instructor! Quick to answer questions, very knowledgeable and gave great examples and stories."
-Katrina Howard,
Booz Allen & Hamilton

"Once again, SANS has exceeded my expectations and successfully re-focused my view of threats and risks. I recommend this course because it is very enlightening."
-Charles Allen,
EM Solutions, Inc.

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

FORENSICS 508

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Oct 5 - Sat, Oct 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jake Williams

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

digital-forensics.sans.org

"Real-case examples and talking about real-world "best-practice" is most valuable. Class discussions and questions were the best part of learning the material."
-Davie Yeo, Alvarez & Marcel

"FOR508 is an extremely valuable course overall. It brings essential topics into one class and covers an extensive amount of topics along with excellent reference material."
-Edgar Zayas, U.S. Securities and Exchange Commission

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

- How the breach occured
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

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.

Who Should Attend

- Incident Response Team Leaders and Members
- Security Operations Center (SOC) personnel and Information Security Practitioners
- Experienced Digital Forensic Analysts
- System Administrators
- Federal Agents and Law Enforcement
- Red Team Members, Penetration Testers, and Exploit Developers
- SANS FOR408 and SEC504 Graduates

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.

GCFA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

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

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

Jake Williams *SANS Certified Instructor*

Jake Williams is a technical analyst with the Department of Defense (DoD) where he has over a decade of experience in systems engineering, computer security, forensics, and malware analysis. Jake has been providing technical instruction for years, primarily with HBGary, where he was the principal courseware developer and instructor for their products. He also maintains malware reverse engineering courses for CSRgroup Computer Security Consultants. Recently, he has been researching the application of digital forensic techniques to public and private cloud environments. Jake has been involved in numerous incident response events with industry partners in various consulting roles. Jake led the winning government team for the 2011 and 2012 DC3 Digital Forensics Challenge. He has spoken at numerous events, including the ISSA events, SANS @Night, the DC3 conference, Shmoocon, and Blackhat. @MalwareJake

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:

What's New for Security in Windows 10 and Server 2016?

Jason Fossen

Windows 8 was a flop, worse than Vista, so will Windows 10 be successful? The return of the Start Menu, touch screen integration, the faster Edge browser, and Cortana should make Windows 10 popular with users. Windows 10 also includes significant changes for security and manageability in large organizations, such as "Windows as a Service" rolling updates and deeper integration with Azure Active Directory. In this lively talk, Jason Fossen, author of the Securing Windows (SEC505) course at SANS, will lay out what to love and fear in Windows 10 and Windows Server 2016. We will also talk about some of the epic changes going on at Microsoft, now that CEO Steve Ballmer is gone. Is it really a new era for Microsoft? Come join the presentation and see what Microsoft is betting its future on!

DIY vulnerability discovery with DLL Side Loading

Jake Williams

In this talk, Jake (contributing author on FOR526, FOR610, and SEC760) will teach you how to discover vulnerabilities like a rock star using DLL side loading. This technique (ab)uses the way Windows searches for DLLs to load into a program. The behavior is nearly laughable and introduces serious risks, especially when developers don't understand filesystem permissions. Attackers know this and use it for privilege escalation and stealthy persistence. Once you understand how DLL side loading works, you'll be able to find it in your next investigation. Plus you'll look like a infosec rock star when you find vulnerabilities in your organization's custom software.

SANS 8 Mobile Device Security Steps

Chris Crowley

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

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 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.

FUTURE SANS TRAINING EVENTS

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

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

SANS Boston 2015
Boston, MA | August 3-8 | #SANSBoston

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

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

SANS South Florida 2015
Fort Lauderdale, FL | November 9-14 | #SANSFLA

SANS Pen Test Hackfest SUMMIT & TRAINING
Washington, DC | November 16-23

SANS San Francisco 2015
San Francisco, CA | November 30 - December 5 | #SANS-SanFran

SANS Security Leadership SUMMIT & TRAINING
Dallas, TX | December 3-10

SANS Cyber Defense Initiative 2015
Washington, DC | December 12-19 | #SANSCDI

SANS SEATTLE 2015

Hotel Information

Training Campus

Renaissance Seattle Hotel

515 Madison Street
Seattle, WA 98104
800.546.9184
sans.org/event/seattle-2015/location

Escape to the Renaissance Seattle Hotel, a stylish hotel in Seattle conveniently located just minutes from Pike Place Market and upscale shopping. There is always something wonderfully new to discover while staying at this hotel. Unwind in spacious guest rooms with stunning views of Puget Sound, the mountains and city skyline. Enjoy casual dining coupled with spectacular city views at R View, a premier Seattle hotel restaurant. Come discover how this hotel seamlessly combines luxury, comfort and technology into an unforgettable urban retreat.

Special Hotel Rates Available

A special discounted rate of $179.00 S/D will be honored based on space availability.
Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high speed Internet in your room and are only available through Sept. 4, 2015.

Top 5 reasons to stay at the Renaissance Seattle Hotel

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Renaissance Seattle Hotel, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Renaissance Seattle Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS SEATTLE 2015

Registration Information

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

Register online at sans.org/event/seattle-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	**8/12/15**	**$400.00**	**9/2/15**	**$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 September 16, 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 Portal
Account
Sign up for a
SANS Portal
Account
and receive free
webcasts, newsletters,
the latest news and
updates, and many other
free resources.
sans.org/account