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

SANS Scottsdale 2017

February 20-25

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Eight courses on

Cyber Defense

Penetration Testing

Incident Response

Digital Forensics

Ethical Hacking

Management

SAVE $400

Register and pay by Dec 28th – Use code **EarlyBird17**

GIAC
GIAC-Approved Training

"At SANS the technical level of expertise is hard to match, and they offer a range of courses simply not available anywhere else."

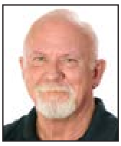
-Eric Jernigan, Genesis Financial Solutions

www.sans.org/scottsdale

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Scottsdale 2017 lineup of instructors includes:

Chris Christianson
SANS Instructor
@cchristianson



Paul A. Henry
Senior Instructor
@phenrycissp

David Hoelzer
Faculty Fellow
@it_audit

Rob Lee
Faculty Fellow
@robtlee
@sansforensics

My-Ngoc Nguyen
Certified Instructor
@MenopN

Ed Skoudis
Faculty Fellow
@edskoudis

John Strand
Senior Instructor
@strandjs

Johannes Ullrich, PhD
Senior Instructor
@johullrich

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: ***If I Wake Evil!!!*** – John Strand

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

Exploitation 101: Stacks, NX/DEP, ASLR and ROP! – David Hoelzer

The Red Pill. Become Aware: Squashing Security Misconceptions and More
My-Ngoc Nguyen

Save $400 when you register and pay by Dec 28th using code EarlyBird17

Courses-at-a-Glance

<table>
<tr><th></th><th></th><th>MON 2-20</th><th>TUE 2-21</th><th>WED 2-22</th><th>THU 2-23</th><th>FRI 2-24</th><th>SAT 2-25</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security</td><td colspan="5">Page 1</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">Page 2 SIMULCAST</td></tr>
<tr><td>SEC503</td><td>Intrusion Detection In-Depth</td><td colspan="6">Page 3</td></tr>
<tr><td>SEC504</td><td>Hacker Tools, Techniques, Exploits, and Incident Handling</td><td colspan="6">Page 4 SIMULCAST</td></tr>
<tr><td>SEC560</td><td>Network Penetration Testing and Ethical Hacking</td><td colspan="6">Page 5 SIMULCAST</td></tr>
<tr><td>SEC566</td><td>Implementing and Auditing the Critical Security Controls – In-Depth</td><td colspan="5">Page 6</td><td></td></tr>
<tr><td>FOR408</td><td>Windows Forensic Analysis</td><td colspan="6">Page 7</td></tr>
<tr><td>MGT512</td><td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td><td colspan="5">Page 8</td><td></td></tr>
</table>

Register today for SANS Scottsdale 2017!
www.sans.org/scottsdale

@SANSInstitute
Join the conversation:
#SANSScottsdale

SANS

SEC301:

Intro to Information Security

Five-Day Program
Mon, Feb 20 - Fri, Feb 24
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge but are new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Authored by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp Style**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

GIAC Information Security Fundamentals GISF
www.giac.org/gisf

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

"Excellent course for someone who is looking to become a security engineer or to improve existing IT security practices."
-Ansar Khalil, HomeStreet Bank

"I appreciate the step-by-step nature of the labs used as the explanations. They are thorough, relevant, and doable."
-Monique Avery, Seattle PD

My-Ngoc Nguyen *SANS Certified Instructor*

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She has 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been assisting client organizations in both the public and private sectors to implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master's degree in management information systems, she carries top security certifications, including GPEN, GCIH, GSEC, and CISSP and is a former QSA. She is an active member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc co-founded the non-profit public service organization CyberSafeNV to raise security awareness among Nevada residents and is presently the organization's chairperson. @MenopN

SEC401:
Security Essentials Bootcamp Style

Six-Day Program
Mon, Feb 20 - Sat, Feb 25
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Paul A. Henry

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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*!

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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

ALSO AVAILABLE VIA SIMULCAST

See page 13 for details.

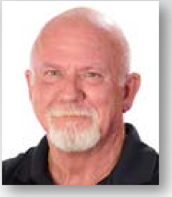
www.giac.org/gsec

www.sans.edu

www.sans.org/8140

BUNDLE ONDEMAND WITH THIS COURSE
www.sans.org/ondemand

> "The training was valuable and has made me more aware of the evil that lurks in the cyber world. Now I can take preventative measures."
> -Anna Gonzales, Brazosport College



Paul A. Henry *SANS Senior Instructor*

Paul 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. He 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. @phenrycissp

SEC503:

Intrusion Detection In-Depth

Six-Day Program
Mon, Feb 20 - Sat, Feb 25
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 (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You 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.

"It is invaluable to get real-world examples from professionals currently working in this field as well as teaching it."
-Mike Heymann, EOG Resources

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.

www.giac.org/gcia

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

"Johannes is very good at explaining details on how tools work. He is very good at what he does, and has lots of great knowledge and experience."
-Ryan Hunt, Alert Logic

Johannes Ullrich, PhD *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Feb 20 - Sat, Feb 25
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

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

"Great instruction! SEC504 covered topics very thoroughly and gave great examples."
-Kevin H., U.S. Department of Homeland Security

This course enables you to turn the tables on computer attackers by helping you to 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 attacks. 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.**

"I have had a lot of training and SEC504 with John Strand is the best course I've ever had!"
-Mark S., U.S. Army

ALSO AVAILABLE VIA SIMULCAST

See page 13 for details.

GIAC CERTIFIED INCIDENT HANDLER GCIH
www.giac.org/gcih

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

▶❚❚ Bundle OnDemand with this course
www.sans.org/ondemand

John Strand *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC464: Hacker Detection for System Administrators. John is also the course author for SEC464. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing. @strandjs

SEC560:

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Feb 20 - Sat, Feb 25
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

ALSO AVAILABLE VIA SIMULCAST

See page 13 for details.

www.giac.org/gpen

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

> "This course pulls together all of the tools needed for pen testing in a very clear and logical manner. SEC560 is excellent and highly valuable training!"
> -BILL HINDS,
> PROJECT MANAGEMENT INSTITUTE

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with **over 30 detailed hands-on labs** throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently…and masterfully.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. **You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.**

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis has taught cyber incident response and advanced penetration testing techniques to more than 12,000 cybersecurity professionals. He is the lead for the SANS Penetration Testing Curriculum. His courses distill the essence of real-world, front-line case studies because he is consistently one of the first experts brought in to provide after-attack analysis of major breaches where credit card and other sensitive financial data is lost. Ed led the team that built NetWars, the low-cost, widely used cyber training and skills assessment ranges relied upon by military units and corporations with major assets at risk. His team also built CyberCity, the fully authentic urban cyber warfare simulator that was featured on the front page of the *Washington Post.* He was the expert called in by the White House to test the security viability of the Trusted Internet Connection (TIC) that now protects U.S. government networks and to lead the team that first publicly demonstrated significant security flaws in virtual machine technology. He has a rare capability to translate advanced technical knowledge into easy-to-master guidance, as evidenced by the popularity of his step-by-step *Counter Hack* books. @edskoudis

SEC566:

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
Mon, Feb 20 - Fri, Feb 24
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Chris Christianson

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks, (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

"Excellent use of cases and very applicable, and I will be able to directly apply the lessons to my organization." -Dominic N., Bechtel Marine

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

"Great course! Nice blend of practical, policy, realistic, and idealistic."
-Amy Bennett, NOAA

GIAC CRITICAL CONTROLS CERTIFICATION
GCCC
www.giac.org/gccc

SANS Technology Institute
www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

Chris Christianson *SANS Instructor*

Chris Christianson is an Information Security Consultant based in Northern California. He has 20 years of experience in the field and many technical certifications, including the CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, GWAPT, and GISF. He holds a Bachelor of Science degree in management information systems and he has served as the Assistant Vice President in the Information Technology department at one of the nation's largest credit unions. Chris has also been an expert speaker at conferences, and has contributed to numerous industry articles. @cchristianson

FOR408:
Windows Forensic Analysis

Six-Day Program
Mon, Feb 20 - Sat, Feb 25
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

www.giac.org/gcfe

www.sans.edu

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

"The Windows registry forensic section blew my mind! I didn't think it stored that much information."
-Tung Nguyen, Denver Water

"Rob's depth of knowledge and enthusiasm for the subject is unparalleled!"
-Glyn Gowing, PhD, Michelin

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.

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 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.

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

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. 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

SANS

MGT512:
SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, Feb 20 - Fri, Feb 24
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: David Hoelzer

GIAC SECURITY LEADERSHIP CERTIFICATION GSLC
www.giac.org/gslc

SANS Technology Institute
www.sans.edu

www.sans.org/8140

▶❚❚
BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

> "David is one of the best instructors, giving worthwhile information while engaging the students."
> -MELANIE WRIGHT, ALERT LOGIC

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. In addition, the course has been engineered to incorporate the NIST Special Publication 800 series guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

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.

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

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!

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring SANS Fellow instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow at the Center for Cybermedia Research and at the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @it_audit

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:

If I Wake Evil!!!

John Strand

Let's say I went to the dark side to get their sweet sweet cookies... Let's say that all goodness had left me... How would I attack you? This talk will answer that question. It will also show you how to stop me.

Welcome Threat Hunters, Phishermen, and Other Liars

Rob Lee

Over the past few years, a 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 exactly what it is and 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 into something more than the loose definition of "find evil," primarily due to the massive amount of incident response data currently collected about our attackers. These data have 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.

Exploitation 101: Stacks, NX/DEP, ASLR, and ROP!

David Hoelzer

In this two-hour talk we will begin with basic stack overflows and then introduce the various protections one at a time... and demonstrate how they are defeated! The talk will cover stack overflows, bypassing DEP/NX (non-executable stacks), defeating ASLR and defeating code signing with ROP. While the talk covers technical topics, even those with less of a technical background will walk away with an appreciation of just how easy exploit development actually is!

The Red Pill. Become Aware: Squashing Security Misconceptions and More

My-Ngoc Nguyen

"You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in wonderland, and I show you how deep the rabbit hole goes."
-Morpheus, to Neo in The Matrix

Take the red pill, come join us down this rabbit hole, and get your head out of the sand to better protect yourself, your company/organization, and the things that matter to you (e.g., your loved ones, your finances, your identity). In this presentation, you will get insights on common misconceptions and trends that led to many breaches, especially those that made headlines. We'll touch on some details from those headline breaches to show commonalities, address the main misconceptions, describe attackers' approaches, provide some statistics, and most importantly, provide helpful tips for all members of the audience.

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days

of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an **OnDemand Bundle**

- 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.

Get Certified with **GIAC Certifications**

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS SECURING THE HUMAN

Security Awareness Training by the Most Trusted Source

Computer-based Training for Your Employees

End User
CIP v5/6
ICS Engineers
Developers
Healthcare

- Let employees train on their own schedule
- Tailor modules to address specific audiences
- Courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes

Visit SANS Securing The Human at
securingthehuman.sans.org

Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand

SANS Technology Institute

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

Master's Degree Programs:

► M.S. in Information Security Engineering
► M.S. in Information Security Management

Specialized Graduate Certificates:

► Cybersecurity Engineering (Core)
► Cyber Defense Operations
► Penetration Testing and Ethical Hacking
► Incident Response

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

GI Bill.

Eligible for veterans education benefits!
Earn industry-recognized GIAC certifications throughout the program.
Learn more at www.sans.edu | info@sans.edu

GIAC

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

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

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Cyber Defense Initiative 2016
Washington, DC | Dec 10-17

Security East 2017
New Orleans, LA | Jan 9-14

Las Vegas 2017
Las Vegas, NV | Jan 23-30

Cyber Threat Intelligence
SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

SOUTHERN CALIFORNIA
Anaheim 2017
Anaheim, CA | Feb 6-11

Dallas 2017
Dallas, TX | Feb 27 - Mar 4

San Jose 2017
San Jose, CA | Mar 6-11

Tysons Corner Spring 2017
McLean, VA | Mar 20-25

ICS Security
SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27

Pen Test Austin 2017
Austin, TX | Mar 27 - Apr 1

SANS 2017
Orlando, FL | Apr 7-14

Threat Hunting and IR
SUMMIT & TRAINING 2017
Orlando, FL | Apr 18-25

Baltimore Spring 2017
Baltimore, MD | Apr 24-29

Automotive Cybersecurity
SUMMIT & TRAINING 2017
Detroit, MI | May 1-8

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

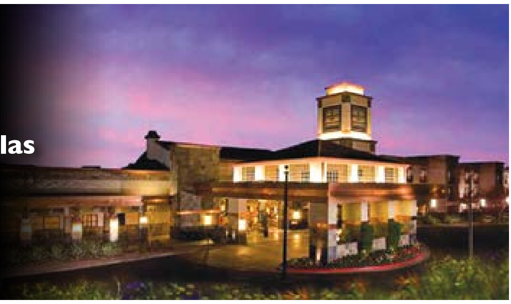
SANS SCOTTSDALE 2017

Hotel Information

Training Campus

Hilton Scottsdale Resort and Villas

6333 North Scottsdale Road
Scottsdale, AZ 85250
480-948-7750
www.sans.org/event/scottsdale-2017/location



Hilton Scottsdale Resort & Villas is located in the heart of Scottsdale, Arizona, within minutes of shopping, dining, world-class golf, and business districts. Set in the shadow of the majestic Camelback Mountain, this AAA Four Diamond Scottsdale resort combines a relaxed ambiance with decor inspired by the Sonoran Desert.

Special Hotel Rates Available

A special discounted rate of $229.00 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 January 27, 2017.

Top 5 reasons to stay at Hilton Scottsdale Resort and Villas

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 Hilton Scottsdale Resort and Villas, 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 Hilton Scottsdale Resort and Villas that you won't want to miss!

5 Everything is in one convenient location!

SANS SCOTTSDALE 2017

Registration Information

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

Register online at www.sans.org/scottsdale

Select your course 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 **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	12-28-16	$400.00	1-18-17	$200.00

Some restrictions apply.

SANS SIMULCAST

To register for a SANS Scottsdale 2017 Simulcast course, please visit www.sans.org/event/scottsdale-2017/attend-remotely

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.

www.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 February 1, 2017 – processing fees may apply.

Open a **SANS 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 FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code "EarlyBird17" before December 28th.

www.sans.org/scottsdale

BROCHURE CODE

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address. NALT-BRO-Scottsdale-2017