THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Scottsdale 2015

Scottsdale, AZ | February 16-21

"This was my first SANS course, and I didn't know what to expect. Now that I've been through the course, I must say the experience was fantastic."

-Gary Hughes, Seagate Technology

Choose from these popular courses:

Continuous Monitoring and Security Operations ***NEW!***

Security Essentials Bootcamp Style

Network Penetration Testing and Ethical Hacking

Windows Forensic Analysis

Advanced Security Essentials - Enterprise Defender

Implementing and Auditing the Critical Security Controls - In-Depth

IT Security Strategic Planning, Policy and Leadership

GIAC Approved Training

Save $400
by registering early!
See page 13 for more details.

REGISTER AT **sans.org/event/scottsdale-2015**

SANS' exceptional training is returning to **Scottsdale in 2015** from **February 16-21**. Once again we bring our top courses in IT security, pen testing, computer forensic analysis, and security management. Also in our lineup is our new course, ***SEC511: Continuous Monitoring and Security Operations***. Our instructors for Scottsdale, Dr. Eric Cole, Ed Skoudis, Seth Misenar, Randy Marchany, Keith Palmgren, Mike Pilkington, and Mark Williams are real-world practitioners who will ensure that what you learn in class will be up-to-date information and that you will be able to apply your information security training the day you get back to the office!

Do you want to earn an advanced degree in information security? **SANS Technology Institute** offers a Master of Science degree in Information Security Engineering (MSISE) or Information Security Management (MSISM). Also, learn more about the new graduate certificates in penetration testing and ethical hacking, incident response, or cybersecurity engineering. For more information see sans.edu and apply today.

Five of our seven courses offered are associated with **GIAC Certifications**, and two certifications align with **DoD Directive 8570**. To learn more, visit giac.org and register for your certification attempt.

This brochure includes comprehensive course descriptions, instructor bios, and information on the bonus sessions including: special events, keynote speaker, and evening talks that will keep you informed about the latest information and the forces shaping cybersecurity. These sessions are open to all paid attendees at no additional cost.

Our SANS Scottsdale 2015 location is the **Hilton Scottsdale Resort & Villas** in the heart of the city. This hotel has majestic views of Camelback Mountain, with an elevation of 2,704 feet this mountain is excellent for hiking or climbing. Take a jeep tour through the Sonoran desert, play a round of golf at a championship golf course, stroll underneath hot-house flowers at the Desert Botanical Garden or enjoy the shopping at Scottsdale Fashion Square Mall, Arizona's largest mall. And remember, Scottsdale's average high temperature in February is 73 degrees, so this might be a nice winter break.

A special discounted rate of $189.00 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 21, 2015. See our registration page for complete information.

For the best discount, register and pay by December 24 and save up to $400 on tuition fees. Start making your training and travel plans now, and let your colleagues and friends know about SANS Scottsdale 2015. We look forward to seeing you there.

SANS

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

"I have taken multiple SANS courses and the virtual image for this course seemed most polished and everything just worked. Good course test apps as well."
-Feliz Simmons, AIG

"Course content is extremely valuable for use in real-world application and directly pertinent to analysis conducted in my lab. It is great to go to a class that I will be able to utilize nearly everything that was taught."
-H. Polend, VA Department of Forensic Science

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

Courses-at-a-Glance

		MON 2/16	TUE 2/17	WED 2/18	THU 2/19	FRI 2/20	SAT 2/21
SEC401	Security Essentials Bootcamp Style	Page 2					
SEC501	Advanced Security Essentials - Enterprise Defender	Page 3					
SEC511	Continuous Monitoring and Security Operations	Page 4					
SEC560	Network Penetration Testing and Ethical Hacking	Page 5					
SEC566	Implementing and Auditing the Critical Security Controls	Page 6					
FOR408	Windows Forensic Analysis	Page 7					
MGT514	IT Security Strategic Planning, Policy and Leadership	Page 8					

@SANSInstitute *Join the conversation:* #SANSScottsdale

Fund Your SANS Training: How to Persuade Your Employer

EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the *Career Roadmap* (sans.org/media/security-training/roadmap.pdf) to arm yourself with all the necessary materials to make a good case for attending a SANS training event.

RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Describe how your knowledge will allow you to become an expert resource for the rest of your team.

VALIDATE

- Earn a GIAC certification, proving to your employer that you gained the expertise they paid for!
- Hone your skills at NetWars and report your competitive score (available free with 5- or 6-day courses at live training events).

SAVE

- The earlier you sign up and pay, the more you save, so explain the benefit of paying up early.
- Save even more with group discounts, or bundled course packages! See inside for details.

ADD VALUE

- Share with your boss that you can add value to your enterprise by meeting with network security experts – people who face the same type of challenges that you face every single day.
- Explain how you will be able to get and share great ideas on improving your IT productivity and efficiency.
- Enhance your SANS training experience with *SANS@Night* talks and the *Vendor Expo*, which are free and only available at live training events.

ALTERNATIVES

- If time out of the office is limited, pitch SANS OnDemand, Event Simulcast, or Live Online Training.
- Highlight that students in our online courses earn the same GIAC scores as those who take training live!

ACT

- With the fortitude and initiative you have demonstrated thus far, you can confidently seek approval to attend SANS training!

Return on Investment

SANS training events are recognized as the best place in the world to get information security education. With SANS, you will 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:

SANS is your first and best choice for information and software security training. The SANS Promise is "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, Feb 16 - Sat, Feb 21
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Dr. Eric Cole

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

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. Our 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?**

giac.org

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.

sans.edu

sans.org/cyber-guardian

"This course gives me a much better understanding of the tools to use to help make networks more secure by pointing out vulnerabilities." -John McDonald, Florida Dept. of LE

sans.org/8570

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"Eric is incredible; he never ceases to amaze me with his ability to relate the information to everyone while keeping the material interesting."
-Brian Ward, Jackson Supply

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including "Hackers Beware," "Hiding in Plain Site," "Network Security Bible," and "Insider Threat." He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. He is a SANS faculty Fellow and course author. @drericcole

SECURITY 501

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Mon, Feb 16 - Sat, Feb 21
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Keith Palmgren
- GIAC Cert: GCED
- Masters Program
- DoDD 8570

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.

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.

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.

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- Students who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want broad, advanced coverage of the core areas to protect their systems
- Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization

"I liked the hands-on with tools to understand how they can be used on both sides of the fence."
-John Watts,
Micron Technology, Inc

"Good exposure to tools, processes, and threats. I enjoyed the real-life business cases that were discussed in class to make the material fresh."
-Lorelei Duff, Lockheed Martin

giac.org

sans.edu

sans.org/8570

Keith Palmgren *SANS Certified Instructor*

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

SECURITY 511

Continuous Monitoring and Security Operations

NEW

SANS

Six-Day Program
Mon, Feb 16 - Sat, Feb 21
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Seth Misenar

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

Who Should Attend

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

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.

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

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

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the capture-the-flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Seth Misenar *SANS Principal Instructor*

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

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Feb 16 - Sat, Feb 21
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

As a cyber security 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 duty head-on.

Who Should Attend

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

THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

The whole course 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 awesome 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, learning about a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. You'll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. 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, wireless, 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.

giac.org

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

With comprehensive coverage of tools, techniques, and methodologies for network, web app, and wireless testing, SEC560 truly prepares you to conduct high-value penetration testing projects end-to-end, step-by-step. Every organization needs skilled infosec personnel who can find vulnerabilities and mitigate their impacts, and this whole course is specially designed to get you ready for that role. 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 masterfully, safely, and efficiently.

sans.edu

sans.org/
cyber-guardian

"The materials in the course directly pertain to my job so having a better understanding of the techniques used against you helps make a better defense. Ed's real-world experiences that he relates in each session are invaluable."
-Tim Dunaway,
U. S. Army Corps of Engineer

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis

SECURITY 566

Implementing and Auditing the Critical Security Controls – In-Depth

SANS

Five-Day Program
Mon, Feb 16 - Fri, Feb 20
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Randy Marchany

- GIAC Cert: GCCC
- Masters Program

giac.org

sans.edu

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Federal agencies or clients
- 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
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

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?

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.

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. Specifically, by the end of the course students will know how to:

- **Create a strategy to successfully defend their data**
- **Implement controls to prevent data from being compromised**
- **Audit systems to ensure compliance with Critical Control standards.**

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.

"This was an awesome course with an amazing amount of material—the capstone did a great job tying it all together."
-D Mayer, Broomfield PD

Randy Marchany *SANS Certified Instructor*

Randy is the Chief Information Security Officer of Virginia Tech and the Director of Virginia Tech's IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. Randy is currently a certfied instructor for the SANS Institute. He is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks of 2000. @randymarchany

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, Feb 16 - Sat, Feb 21
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Pilkington
- GIAC Cert: GCFE
- Masters Program

DFIR
digital-forensics.sans.org

Master Computer Forensics. What Do You Want to Uncover Today?

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

Who Should Attend

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

FOR408: Windows Forensic Analysis focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

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

"The level of knowledge in the field and the real-world examples add a great deal of value."
-Jim Gainor,
Edmonton Police Service

"Knowledgeable and excellent examples that are relative to the material. It provides information that I can use in incident response of investigating unauthorized activities."
-Rick Kozak,
Cubic Transportation Systems

FOR408 Windows Forensic Analysis will teach you to:

- **Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, XP, and Windows Server 2008/2012**
- **Identify artifact and evidence locations that will answer key questions, including questions about program execution, file opening, external device usage, geo-location, file download, anti-forensics, and system usage**
- **Focus your capabilities on analysis instead of how to use a specific tool**
- **Extract key answers by utilizing proper analysis via a variety of free, open-source, and commercial tools in the Windows SIFT Workstation**

GCFE
giac.org

SANS INSTITUTE
sans.edu

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

Mike Pilkington *SANS Instructor*

Mike Pilkington is a senior security consultant for a Fortune 500 company in the oil & gas industry. He has been an IT professional since graduating in 1996 from the University of Texas with a B.S. in Mechanical Engineering. Since joining his company in 1997, he has been involved in software quality assurance, systems administration, network administration, and information security. Outside of his normal work schedule, Mike has also been involved with the SANS Institute as a mentor and instructor in the digital forensics program. @mikepilkington

MANAGEMENT 514

IT Security Strategic Planning, Policy and Leadership

Five-Day Program
Mon, Feb 16 - Fri, Feb 20
9:00am - 5:00pm
30 CPEs
Laptop Recommended
Instructor: Mark Williams
- Masters Program

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but 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.

Who Should Attend

- This course is designed and taught for existing, recently appointed, and aspiring IT and IT security managers and supervisors who desire to enhance their leadership and governance skills to develop their staff into a more productive and cohesive team.

In this course you will learn the entire strategic planning process: what it is and how to do it; what lends itself to virtual teams; and what needs to be done face to face. We will practice building those skills in class. Topics covered in depth include how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's, etc.), historical analysis, mission, vision, and value statements. We will also discuss the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build the roadmap, setting up assessments, and revising the plan.

We will see examples and hear stories from businesses, especially IT and security-oriented businesses, and then work together on labs. Business needs change, the environment changes, new risks are always on the horizon, and critical systems are continually exposed to new vulnerabilities. Strategic planning is a never-ending process. The planning section is hands-on and there is exercise-intensive work on writing, implementing, and assessing strategic plans.

Another focus of the course is on management and leadership competencies. 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. However, leaders and followers influence each other toward the goal – it is a two-way street where all parties perform their functions to reach a common objective.

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. Grooming effective leaders is critical to all types of organizations, as the most effective teams are cohesive units that work together toward common goals with camaraderie and a can-do spirit!

"Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job."
-Ryan Spencer,
Reed Elsevier, Inc.

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experimental knowledge in examples and explanations."
-Sean Hoar,
Davis Wright Tremaine

sans.edu

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of Principal Systems Security Officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During this career Mark has consulted on issues of privacy and security, lead seminars, and developed information security, privacy, and compliance related programs.

SCOTTSDALE BONUS SESSIONS

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given by our instructors and selected subject matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: APT: It is Time to Act *Dr. Eric Cole*

In this engaging talk, one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal, but Detection is a Must."

Privileged Domain Account Protection: How to Limit Credentials Exposure *Mike Pilkington*

In this presentation, I will discuss what you can and cannot do safely with domain accounts. In particular, I will cover attacks against password hashes, security support providers, access tokens, and network authentication protocols.

Information Security Risk Management - No Exceptions! *Mark Williams*

Let me show you how I think that continuous risk assessment and risk management can actually avoid the need for exceptions. By using a logical approach to risk identification, categorization and decision making, you too can do the "impossible" and say: NO EXCEPTIONS!

The 13 Absolute Truths of Security *Keith Palmgren*

Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

Continuous Monitoring - A Practical Example *Randy Marchany*

Continuous monitoring (aka network forensics, extrusion detection, network security monitoring) focuses on monitoring activity on your network and discovering outbound traffic patterns. We assume the network is penetrated and focus on trying to prevent sensitive data from leaving our network. This talk discusses how VA Tech is implementing a CM security architecture on its IPV4 and IPV6 networks.

How to Give the Best Pen Test of Your Life *Ed Skoudis*

In this talk, Ed Skoudis focuses on what we can learn from the hypothetical ultimate pen test that we can directly apply to our real-world pen tests today. Loaded with specific tips, tricks, and strategies, this talk strives to provide actionable advice for all security pros to up their game in providing great penetration tests.

Continuous Monitoring and Real-World Analysis *Seth Misenar*

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

Debunking the Complex Password Myth *Keith Palmgren*

In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home for their users, themselves, and even their children.

SANS NewsBites

Join over 200,000 professionals who subscribe to this high-level, executive summary of the most important news and issues relevant to cyber security professionals. Delivered twice weekly. Read insightful commentary from expert SANS instructors.

Webcasts

SANS Information Security Webcasts are live broadcasts by knowledgeable speakers addressing key issues in cyber security, often in response to breaking risks. Gain valuable information on topics you tell us are most interesting!

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/portal

InfoSec Reading Room

Computer security research and whitepapers

Critical Security Controls

Consensus guidelines for effective cyber defense

Security Policies

Templates for rapid information security policy development

Industry Thought Leadership

In-depth interviews with the thought leaders in information security and IT.

OUCH!

OUCH! is the world's leading, free security awareness newsletter designed for the common computer user. Published every month and in multiple languages, each edition is carefully researched and developed by the SANS Securing The Human team, SANS instructor subject-matter experts and team members of the community. Each issue focuses on and explains a specific topic and actionable steps people can take to protect themselves, their family and their organization.

@RISK: The Consensus Security Alert

@RISK provides a reliable weekly summary of:

1. Newly discovered attack vectors
2. Vulnerabilities with active new exploits
3. Insightful explanations of how recent attacks worked and other valuable data

A key purpose of the @RISK is to provide data that will ensure that the Critical Controls continue to be the most effective defenses for all known attack vectors.

FUTURE SANS TRAINING EVENTS

SANS Cyber Defense Initiative 2014
Washington, DC | December 10-19 | #SANSCDI

SANS Security East 2015
New Orleans, LA | January 16-21 | #SecurityEast

SANS Cyber Threat Intelligence SUMMIT & TRAINING 2015
Washington, DC | February 2-9 | #CTISummit

10TH ANNUAL ICS Security SUMMIT – ORLANDO 2015
Orlando, FL | February 23 - March 2 | #SANSICS

SANS DFIR Monterey 2015
Monterey, CA | February 23-28 | #DFIRMonterey

SANS Cyber Guardian 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS Northern Virginia 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

Visit sans.org for a complete schedule.

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

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

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

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

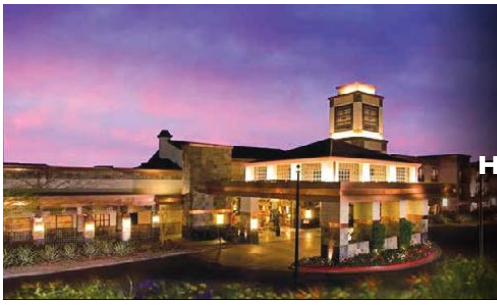
ONLINE TRAINING

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 SCOTTSDALE 2015

Hotel Information

Training Campus

Hilton Scottsdale Resort and Villas

6333 North Scottsdale Road
Scottsdale, AZ 85250
sans.org/event/scottsdale-2015/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 ambience with decor inspired by the Sonoran Desert.

Special Hotel Rates Available

A special discounted rate of $189.00 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 21, 2015. To make reservations for the SANS group rate, go to sans.org/event/scottsdale-2015/location. If you are able to use the Government rate, please call (800) HILTONS (800-445-8667) and ask for the SANS government rate.

Top 5 reasons to stay at the Hilton Scottsdale Resort & 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 the Hilton Scottsdale Resort & 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 the Hilton Scottsdale Resort & Villas that you won't want to miss!
5. Everything is in one convenient location!

SANS SCOTTSDALE 2015

Registration Information

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

Register online at sans.org/event/scottsdale-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.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	12/24/14	$400.00	1/21/15	$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.

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by January 28, 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