THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Capital City 2014

Washington, DC July 7-12

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Intrusion Detection In-Depth

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS® +S™ Training Program for the CISSP® Certification Exam

Implementing and Auditing the Critical Security Controls – In-Depth

Memory Forensics In-Depth

"SANS is the premier cybersecurity training institution."
-Jose Marquez, DIA

GIAC Approved Training

Register at www.sans.org/event/capital-city-2014

Save $400 by registering early!

See page 13 for more details.

You are invited to **Washington, DC** for another outstanding offering of IT security, forensics, and security management courses. It is hard to miss the daily headlines bringing to our attention the many cybersecurity breaches, which means that the need for individuals with IT security qualifications is in high demand. SANS will offer seven courses at the **Capital Hilton on July 7-12**.

Make your plans now to attend SANS Capital City DC 2014 this July for our top courses brought to you by our award-winning instructors. This brochure will provide you with information on course descriptions and instructor bios for Paul A. Henry, Mike Poor, Kevin Fiscus, Jonathan Ham, G. Mark Hardy, Keith Palmgren, and Jake Williams. Our faculty team will ensure that you can use what you learn in the classroom as soon as you return to the office.

Five of our courses are associated with the prestigious *GIAC Certification*. And to fast-track your career, five of our courses may also help you earn your master's degree at the *SANS Technology Institute (STI)*, a regionally accredited, postgraduate institution focused on cybersecurity education. Find out more about GIAC and STI in this brochure.

Add depth to your training experience with unique bonus sessions, including:

- **Keynote: Who's Watching the Watchers?** presented by Mike Poor
- **GIAC Program Overview & SANS Technology Institute Open House**
- **50 Shades of Hidden – Diving Deep Into Code Injection** presented by Jake Williams
- **Weaponizing Digital Currency** presented by G. Mark Hardy
- **Incident Response and Forensics In The Cloud** presented by Paul A. Henry
- **DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls** presented by Kevin Fiscus
- **The 13 Absolute Truths of Security** presented by Keith Palmgren
- **Vendor Showcase events** – Wednesday, July 9

SANS training is well known for being relevant and practical. Our award-winning faculty has proven they understand current challenges and their real-world experience will increase the value of the course material.

Our campus for this event, the *Capital Hilton*, is located just two blocks north of the White House, which rewards guests with all the excitement Washington, DC has to offer — near museums and memorials, theatres and art galleries, shopping, dining, nightlife and other DC attractions, see http://washington.org for more information. A discounted room rate of $199 Single/Double is available to SANS students until June 12, but space is limited so book early!

Register and pay by May 21 and receive a $400 tuition fee discount for any course! Start making your training and travel plans now – let your colleagues and friends know about ***SANS Capital City 2014***!

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

"The resources I learned are priceless, and I gained so much knowledge in one week. Awesome!"
-Craig Bowden, Bowdoin College

"SANS training gives me experience I can use immediately at work and allows for incredible networking opportunities!"
-Mike Saunders, Noridian Mutual Insurance

"SANS presents superior content and the opportunity for certifications."
-Greg Stiger, Oliver Wyman

Courses-at-a-Glance

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, July 7 - Sat, July 12
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Keith Palmgren

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

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems.

This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

"SEC401 highlights many components that often will get overlooked by organizations trying to secure their information and people."
-Claire Kubitzky, APH

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.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
- 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

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.

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, July 7 - Sat, July 12
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor

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

Who Should Attend

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

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the **Intrusion Detection In-Depth** course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches. A more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"Mike is extremely informative and conveys his knowledge effectively."
-Benjamin Smith, USMC

"Mike Poor provides great instruction, very energetic, and interactive."
-Kenneth Drennon, S.C. National Guard

"Mike respects what we are here for and doesn't rush us out at the end of the day. He takes the time to explain any problem areas."
-Aaron Didier, Motorola Solutions

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling "Snort" series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, July 7 - Sat, July 12
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Jonathan Ham

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

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

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

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, 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.

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"As an incident manager, SEC504 gave me a more in-depth look into how incidents occur and the tools to combat such incidents."
-Taylor Overhultz, Bank of America

"SEC504 was a fantastic learning experience. So much information presented in a manner that was understandable."
-Scotlyn Monk, Ingalls Information Security

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian Federal agencies. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response – volunteering and teaching for both the National Ski Patrol and the American Red Cross.

SECURITY 566

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
Mon, July 7 - Fri, July 11
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Kevin Fiscus

Cybersecurity attacks are increasing and evolving so rapidly that 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.

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense (DoD) 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 SEC440, SEC401, SEC501, MGT512, and other SANS Audit courses

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 governments 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.

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.

"SEC566 gave me real-world info that I can begin to implement immediately."
-Dave Nevin,
Oregon State University

"SEC566 is valuable because it helped me understand security-related items that I needed to consider and what the best practices are."
-Scott Kreitzer, The Health Plan of the Upper Ohio Valley, Inc.

"SEC566 is an awesome course! Everything I had hoped for and more!"
-Randy Pauli, Chelan County PUD

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC504, SEC542, SEC560, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children.

FORENSICS 526

Memory Forensics In-Depth

SANS

Five-Day Program
Mon, July 7 - Fri, July 11
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: Jake Williams

Digital Forensics and Incident Response
http://computer-forensics.sans.org

"All manuals should be written like those used in FOR526. Not only do you see the answers, but also know how you got there."
-Barry Friedman, NY Police

"FOR526 is a great deep dive into memory and an excellent tutorial to creating plugins for volatility."
-Karel Nykles, CESNET

"FOR526 helped me to expand my knowledge of host forensics."
-Christopher Courchesne, Man Tech Intl.

Malware Can Hide, But It Must Run

Acquiring and analyzing physical memory is seen by Digital Forensics and Incident Response (DFIR) professionals as critical to the success of an investigation, whether it be a criminal case, employee policy violation, or enterprise intrusion. Investigators who are not looking at volatile memory are leaving evidence on the table. The valuable contents of RAM hold evidence of user actions as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the "smoking gun" that unravels the story of what happened on a system.

Who Should Attend

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- Anyone who plays a part in the acquisition, preservation, forensics, or analysis of Microsoft Windows computers

Just as it is crucial to understand disk and registry structures in order to substantiate findings in traditional system forensics, it is equally critical to understand memory structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the current case. There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. This course takes the DFIR professional through acquisition, validation, and memory analysis with hands-on, real-world, and malware-laden memory images. The course draws on best practices and recommendations from top experts in the DFIR field.

FOR526 provides the critical skills necessary for digital forensics examiners and incident responders to deftly analyze captured memory images and live response audits. By using the most effective freeware and open-source tools in the industry today and delivering a deeper understanding of how these tools work, this five-day course shows DFIR professionals how to unravel the real story of what happened on a system. It is a critical course for any serious investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

Remember: "Malware can hide, but it must run." It is this malware paradox that is the key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible for them to hide their footprints completely from a skilled incident responder performing memory analysis. FOR526 will ensure that you and your team are ready to respond to the challenges inherent in DFIR by using cutting-edge memory forensics tools and techniques.

Jake Williams *SANS Certified Instructor*

Jake Williams is a technical analyst with the Department of Defense (DoD) where he has over a decade of experience in systems engineering, computer security, forensics, and malware analysis. Jake has been providing technical instruction for years, primarily with HBGary, where he was the principal courseware developer and instructor for their products. He also maintains malware reverse engineering courses for CSRgroup Computer Security Consultants. Recently, he has been researching the application of digital forensic techniques to public and private cloud environments. Jake has been involved in numerous incident response events with industry partners in various consulting roles. Jake led the winning government team for the 2011 and 2012 DC3 Digital Forensics Challenge. He has spoken at numerous events, including the ISSA events, SANS @Night, the DC3 conference, Shmoocon, and Blackhat.Jake holds a Bachelor's degree in CIS, a Master's Degree in Information Assurance, and is currently pursuing a PhD in Computer Science. His research interests include protocol analysis, binary analysis, malware RE methods, and methods for identifying malware Command and Control (C2) techniques. He holds numerous certifications, including GREM, GCFE, GSNA, GCIA, GCIH, GCWN, GPEN, RHCSA, and CISSP.

MANAGEMENT 414

SANS® +S™ Training Program for the CISSP® Certification Exam

Six-Day Program
Mon, July 7 - Sat, July 12
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Laptop NOT Needed
Instructor: Paul A. Henry

- GIAC Cert: GISP
- DoDD 8570

Take advantage of SANS CISSP® Get Certified Program currently being offered.

www.sans.org/special/cissp-get-certified-program

Who Should Attend

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

Domain 1: Access Controls
Domain 2: Telecommunications and Network Security
Domain 3: Information Security Governance & Risk Management
Domain 4: Software Development Security
Domain 5: Cryptography
Domain 6: Security Architecture and Design
Domain 7: Security Operations
Domain 8: Business Continuity and Disaster Recovery Planning
Domain 9: Legal, Regulations, Investigations and Compliance
Domain 10: Physical (Environmental) Security

www.giac.org

www.sans.org/8570

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of résumé
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Periodic Audit of CPEs to maintain the credential

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

"MGT414 helped bring important information that I had in my memory to the surface. The course is organized and very informative."
-David Raymond, U.S. Army

"Paul is an excellent instructor – the combination of the knowledge and humor makes learning the material easier."
-Sean Walsh, Riverbed Technology

Paul A. Henry *SANS Senior Instructor*

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

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, July 7 - Fri, July 11
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits
Laptop NOT Needed
Instructor: G. Mark Hardy

- GIAC Cert: GSLC
- Masters Program
- DoDD 8570

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 gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

Who Should Attend

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

Essential security topics covered in this management course 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, 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.

"MGT512 encompasses topics in all security areas. This was my first SANS experience and I greatly enjoyed it. I will certainly advocate to my superiors the value I have received."
-Mark McCready,
Modern Woodmen of America

"MGT512 course material and the instructor were top notch. SANS delivers a quality product every time."
-Charles Brown III,
MCSF-Blount Island

Knowledge Compression™

Knowledge Compression™ is an optional add-on feature to a SANS class which 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!

www.giac.org

www.sans.edu

www.sans.org/8570

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/ Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications.

CAPITAL CITY 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: Who's Watching the Watchers? *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation and aggregation... but do we know if we have it right? Will we detect the NextGen™ attackers? In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

50 Shades of Hidden – Diving Deep Into Code Injection *Jake Williams*

The technological prowess of attackers has increased dramatically over the last several years. Gone are the days when you could hope to discover malware.exe running in the process list. Attackers are migrating to code injection as a method to remain hidden from prying eyes examining process list entries. Sure, we've all heard the term code injection or DLL injection, but what does it really mean? How does it really work? Hint: it isn't magic. However, many explanations are bereft, with hand waving and pressing the "I believe" button. In this webcast, we'll talk about how code injection really works at a more technical level. We'll take a quick look at some malware that's performing code injection and discuss detection strategies for when your antivirus fails to detect it. Code injection is a huge topic and we can't cover every aspect in an hour, but the goal is for you to walk away understanding the basics of what's happening under the hood so you can speak intelligently to the topic.

The 13 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified 13 "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 13 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 13 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.

Weaponizing Digital Currency *G. Mark Hardy*

Satoshi Nakamoto wasn't stupid. In the early days, he (they) mined over 1,000,000 Bitcoins when nobody really cared. If Bitcoin continues to increase in value at the rate it did last year, someone will be holding a massive currency weapon. George Soros destabilized the British pound in 1992 and made over 1,000,000,000 profit. In the largest counterfeiting operation in history, Nazi Germany devised Operation Bernhard to destabilize the British economy by dropping millions of pounds from Luftwaffe aircraft. If the holder of the megabitcoin has a currency digital weapon that works frictionlessly in milliseconds, against whom will he target it? Can it destabilize an entire government? Can it be continuously reused for blackmail? What should governments be doing now to plan for this contingency and fight back? We'll discuss an entirely new class of information weapon – digital cryptocurrency – and how it might either change the course of history, or be relegated to the ash heap of failure.

Incident Response and Forensics In The Cloud *Paul A. Henry*

The move to private and public cloud changes many things, including how we respond for IR and forensics. As an example: traditionally in a physical realm we relied upon imaging a server's hard drive as well as RAM to perform a thorough analysis. Today in the cloud, creating a forensically sound image of an "instance" of a server to capture the server's abstracted hard disk and an image of its RAM brings new technical and legal complications. An additional issue to consider is that some vendors platforms are simply not fully supported by our current IR & forensics tools; today's commercial tools lack the ability to perform any analysis at all on a VMware VMFS file system. Lastly, downloading a large server image may simply be cost prohibitive due to the high bandwidth costs associated with moving data out of the cloud environment. The best course of action may be to perform your analysis within the cloud – however, the methods used in the analysis within the cloud must be forensically sound and as always in computer forensics, they must be repeatable and the result must be the same findings. In this session we will begin to explore the changes that simply must be made to your IR and forensics procedures to properly address IR & forensics in the cloud.

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls *Kevin Fiscus*

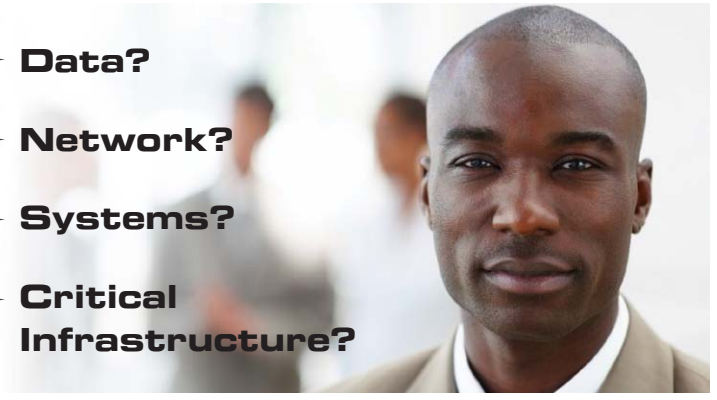
It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

Vendor Showcase

Wednesday, July 9 | 10:30am-10:50am | 12:30pm-1:15pm | 3:00pm-3:20pm

Our events incorporate external vendor partners showcasing some of the best security solutions available. Take advantage of the opportunity to interact with the people behind the products and learn what they have to offer you and your organization.

How Are You Protecting Your



Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification. **Get GIAC certified!**

GIAC offers over 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

Get Certified at
www.giac.org

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Techniques, Exploits, and Incident Handling	GCIH
AUD507	Auditing Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	GSLC

Compliance/Recertification:
To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8570@sans.org or visit www.sans.org/8570

FUTURE SANS TRAINING EVENTS

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

SANS Austin 2014

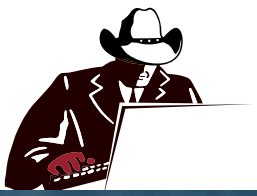
Austin, TX | April 28 - May 3

Security Leadership SUMMIT 2014

Boston, MA | April 29 - May 7

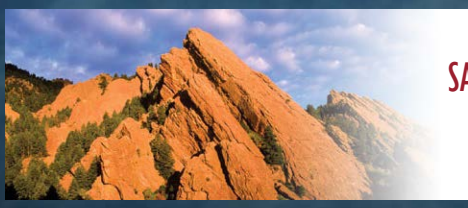
SANS Security West 2014

San Diego, CA | May 8-17



Digital Forensics & Incident Response SUMMIT

Austin, TX | June 3-10

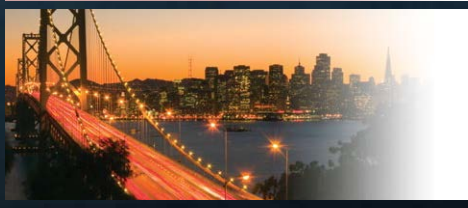


SANS Rocky Mountain 2014

Denver, CO | June 9-14

SANSFIRE 2014

Baltimore, MD | June 21-30



SANS San Francisco 2014

San Francisco, CA | July 14-19

SANS ICS Industrial Control Systems

ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25

SANS Boston 2014

Boston, MA | July 28 - August 2

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

www.sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-learning available anytime, anywhere, at your own pace

www.sans.org/ondemand

vLive

Online, evening courses with SANS' top instructors

www.sans.org/vlive

Simulcast

Attend a SANS training event without leaving home

www.sans.org/simulcast

OnDemand Bundles

Extend your training with an OnDemand Bundle including four months of e-learning www.sans.org/ondemand/bundles

SANS CAPITAL CITY 2014

Hotel Information

Training Campus
Capital Hilton

1001 16th Street NW
Washington, DC 20036
www.sans.org/event/capital-city-2014/location

Special Hotel Rates Available

A special discounted rate of $199.00 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 June 12, 2014. To make reservations, please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

Nestled along the bustle of K Street in downtown Washington, DC, just two blocks north of the White House, gracious hospitality awaits guests at the historic Capital Hilton hotel. The hotel has a thoughtful blend of refreshed, contemporary surroundings and luxurious modern conveniences.

Top 5 reasons to stay at the Capital Hilton

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 Capital Hilton, 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 Capital Hilton that you won't want to miss!
5. Everything is in one convenient location!

SANS CAPITAL CITY 2014

Registration Information

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

Register online at www.sans.org/event/capital-city-2014/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	**5/21/14**	**$400.00**	**6/4/14**	**$250.00**

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 www.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 June 18, 2014 – 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.
www.sans.org/vouchers