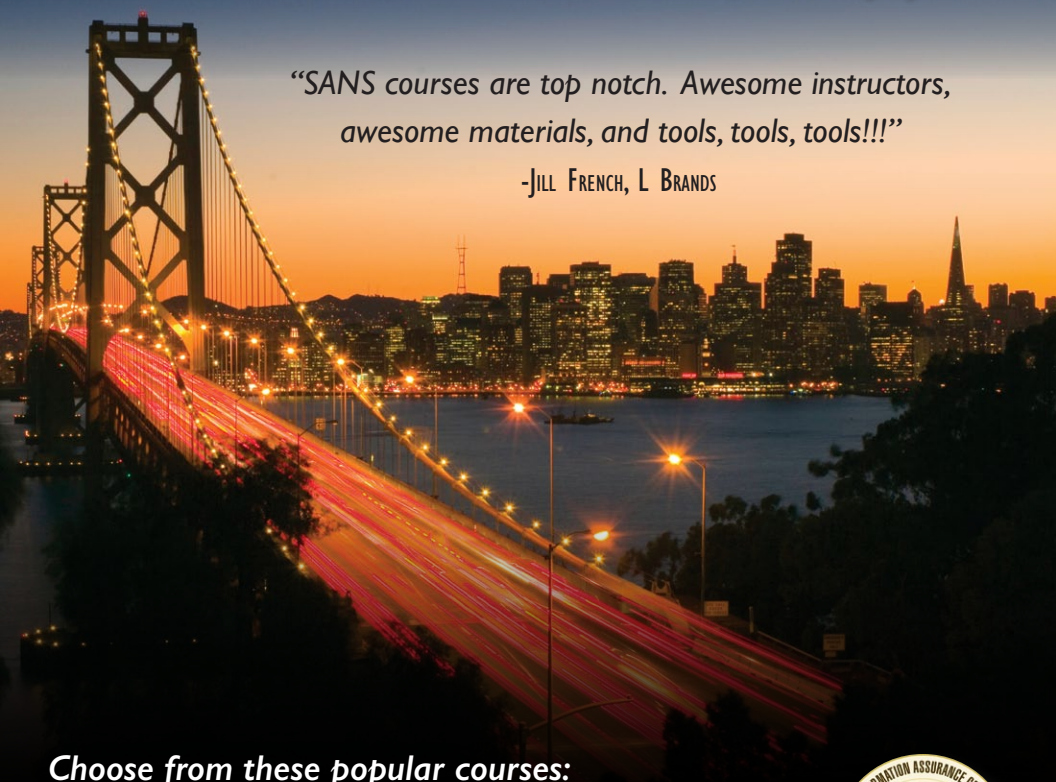
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS San Francisco 2014

San Francisco, CA July 14-19



"SANS courses are top notch. Awesome instructors, awesome materials, and tools, tools, tools!!!"

-Jill French, L Brands

Choose from these popular courses:

Advanced Smartphone Forensics NEW!

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

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

Virtualization and Private Cloud Security

Implementing and Auditing the Critical Security Controls – In-Depth

IT Security Strategic Planning, Policy, and Leadership

GIAC Approved Training

Register at www.sans.org/event/san-francisco-2014

Save $400 by registering early!

See page 13 for more details.

Welcome to SANS San Francisco 2014! It seems with each passing day we learn of more network intrusions, data exfiltration, new vulnerabilities and new threat vectors. As information security professionals you are well-aware of the need for highly relevant and actionable training from real-world security practitioners to help keep your organizations secure and your career on an upward track. That's precisely why this year's SANS San Francisco is important and exciting at the same time.

Register and pay by May 28 to save up to $400 on tuition fees.

SANS San Francisco 2014 features the right mix of courses for today's security challenges including our two most popular security courses SEC401 and SEC504; (NEW!) FOR585: Smartphone Forensics; SEC566: Implementing the Critical Security Controls; SEC579: Virtualization and Cloud Security; MGT514: IT Security Strategic Planning; and, the course I'm teaching, MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam.

The faculty for SANS San Francisco includes Stephen Northcutt and Frank Kim, Paul A. Henry, Dave Shackleford, Stephen Sims, Mark Baggett, Randy Marchany, and Cindy Murphy. These expert instructors understand the challenges you face on a daily basis as their real-world experience increases the value of the course material.

In addition to these great courses and outstanding instructors, SANS San Francisco features SANS@Night presentations and the keynote I'll deliver titled, "Aligning Your Defenses with Today's Evolving Threats." For the complete list of Bonus Sessions, see: www.sans.org/event/san-francisco-2014/bonus-sessions.

Although I am now a senior SANS instructor, I'm a veteran SANS student myself. I took my first SANS course some 20 years ago, and I can say from personal experience that SANS training can both shape and advance your career. The practical skills I gained from my SANS training over the years has enabled me to stay ahead of the curve, to stand out from the crowd and to accelerate my career growth. SANS training can do the same for your career.

In this brochure you will find details on the DoD 8570 Directive, how GIAC certifications are trusted by companies and government agencies, and which of these courses in San Francisco might apply to a SANS Technology Institute master's degree. SANS Technology Institute is the only accredited graduate institution focused solely on cybersecurity.

Our campus for this event, the Hilton San Francisco Union Square, has a special discounted SANS rate of $219 Single/Double, which will be honored based on space availability. Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through June 23, 2014. See our Hotel Information page for all the information you need.

I am excited to be returning to San Francisco with SANS and with you. I hope you will join me and your peers and discover why SANS is the most recognized, respected and trusted information security training in the world. Register today for SANS San Francisco 2014.

Paul A. Henry
Senior SANS Instructor
MCP+I, MCSE, CCSA, CCSE, CISSP-ISSAP, CISM, CISA, CIFI, CCE, ACE, GCFE, MCP+GCFA, GSEC, VCP4/5, vExpert

Paul A. Henry

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

"The instructors are extremely knowledgeable. They have real-world experience so they are able to provide lots of useful examples about the industry."
-Lachlon Walsh, Defence

"SANS has an excellent mix of training, and the instructors have real-world stories, and depth/breadth of experience."
-Larry Dingmore, Click Bank

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

SANS, awarded "Best Professional Training Program" by SC Magazine for 2014, can help you accomplish your cybersecurity career goals!

Courses-at-a-Glance

		MON 7/14	TUE 7/15	WED 7/16	THU 7/17	FRI 7/18	SAT 7/19
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC504	Hacker Techniques, Exploits, and Incident Handling	Page 2					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	Page 3					
SEC579	Virtualization and Private Cloud Security	Page 4					
FOR585	Advanced Smartphone Forensics *NEW!*	Page 5					
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam	Page 6					
MGT514	IT Security Strategic Planning, Policy, and Leadership	Page 7					

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, July 14 - Sat, July 19
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Stephen Sims

- 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.

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

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.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"SEC401 is my first SANS course and I really liked the detail and real-world examples discussed during class."
-Princy John, Trinity Health

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, July 14 - Sat, July 19
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Mark Baggett

- 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

"As a director of IT, SEC504 showed me what my security team should be doing."
-Brian Bounds, Texas Biomedical Research Institute

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

Mark Baggett *SANS Certified Instructor*

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. He has served in a variety of roles from software developer to Chief Information Security Officer. Mark is the author of SANS Python for Penetration testers course (SEC573) and the pyWars gaming environment. Mark teaches several classes in SANS Penetration Testing curriculum including SEC504 (Incident Handing), SEC560 (Penetration Testing) and his Python course. Mark is very active in the information security community. Mark is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. As part of the Pauldotcom Team, Mark generates blog content for the "pauldotcom.com" podcast . In January 2011, Mark assumed a new role as the Technical Advisor to the DoD for SANS. Today he assists various government branches in the development of information security training programs.

SECURITY 566

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
Mon, July 14 - Fri, July 18
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Randy Marchany

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.

"I enjoyed the juxtaposition of how to implement the controls and also how to audit the controls as presented in SEC566."
-Brad Griffin, Ardent Health

"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.

"Randy is a great instructor and his knowledge base is amazing."
-Wendy Ruiz, LLNL

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.

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program
Mon, July 14 - Sat, July 19
9:00am - 5:00pm
Laptop Required
36 CPE/CMU Credits
Instructor: Dave Shackleford

One of today's most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management for virtualized systems. There are even security benefits of virtualization – easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructures.

Who Should Attend

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds – internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

"AWESOME class thus far. I will be able to take a lot back to apply to our Hyper-V environment!!!"
-Craig VanHuss, Crutchfield Corp.

"Class continues to be spot-on. I'm really enjoying class and taking a lot from it as it's forcing me to think about architectural items we hadn't considered as an organization."
-Glenn Galang,
Lake Villa District Library

"SANS training experience is awesome, and valuable for security professionals and operational teams."
-Ken Langley,
UNC School of Medicine

Dave Shackleford *SANS Senior Instructor*

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

FORENSICS 585

Advanced Smartphone Forensics

NEW

SANS

Six-Day Program
Mon, July 14 - Sat, July 19
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Cindy Murphy

It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individuals movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, or detectives
- IT auditors
- SANS SEC575, FOR563, FOR408, and FOR508 graduates looking to take their skills to the next level

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

FOR585: Advanced Smartphone Forensics focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. FOR585, originally conceptualized by Eoghan Casey, Heather Mahalik, and Terrance Maguire, addresses todays smartphone technologies and threats by studying real-life investigative scenarios. Dont miss the NEW FOR585!

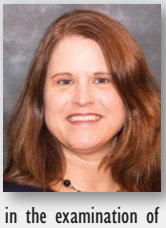
The hands-on exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones. This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensic professionals. Its time to get smarter!

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU

"SANS courses have made me want to eat, sleep, and breath security and forensics!"
-Cory Flynn, Firewall Experts

"If you want to prepare the inevitable considering taking FOR585."

"FOR585 is the best out there."



Cindy Murphy *SANS Instructor*

Detective Cindy Murphy works for the City of Madison, WI Police Department and has been a Law Enforcement Officer since 1985. She is a certified forensic examiner (EnCE, CCFT, DFCP), and has been involved in computer forensics since 1999. She earned her MSc in Forensic Computing and Cyber Crime Investigation through University College, Dublin in 2011. She has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also a part time digital forensics instructor at Madison College, and a part time Mobile Device Forensics instructor for the SANS Institute.

MANAGEMENT 414

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

Six-Day Program
Mon, July 14 - Sat, July 19
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

"The exercise workbooks have truly expanded my knowledge and will indeed be key for studying for the cert."
-Kimberly Harris, BCBSMS

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

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.

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 514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, July 14 - Fri, July 18
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Recommended
Instructors: Stephen Northcutt
Frank Kim

- 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.

The third 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.

Frank Kim

SANS Certified Instructor

Frank Kim is a security leader with over 16 years of experience in information security, risk management, and enterprise IT. He has a passion for developing security strategies and building teams focused on practical solutions to business risks. He currently serves as the curriculum lead for application security at the SANS Institute and is the author and an instructor for the Secure Coding in Java course. Frank is a popular public speaker and has presented at security, software development, and leadership events around the world.

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and served as president of the SANS Technology Institute. Stephen is author/coauthor of Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security 2nd Edition, IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials and Network Intrusion Detection 3rd Edition. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings.

www.sans.edu

SAN FRANCISCO 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: Aligning Your Defenses with Today's Evolving Threats

Paul A. Henry

Defense is an arms race with hackers that are continuously evolving their attack vectors and methods to take advantage of our current weaknesses. Many have fallen into today's "crowd mentality" trap and due diligence has been reduced to simply doing what everyone else is doing. We need to think out of the box and get ahead of the crowd – by gaining an understanding of current threats and attack vectors to realign our defenses. This presentation reviews some of the most current headline grabbing attacks and discusses defenses to provide real risk mitigation.

The best path forward is most often driven by studying recent events. We will take a deep dive in to the Target breach and discuss mitigations in depth.

Introduction to IDA Pro and Debugging

Stephen Sims

In this presentation, Stephen will discuss the most commonly used features and plugins for IDA Pro and WinDbg from an exploitation perspective. You will learn about IDA navigation, IDAPython and IDC scripting, remote debugging, and Kernel debugging. The presentation will be 50% lecture and 50% demonstration. Feel free to bring a demo or licensed version of IDA and WinDbg to play along.

Malware Reloaded

Mark Baggett

Detecting and removing malware is a critical part of every incident response. But that task is getting more and more difficult as attackers continue to "up their game". You remove the malware and scan your hard drive with dozens of anti-malware products, but somehow the attackers keep coming back. Join Mark Baggett for this demonstration packed discussion of malware persistence and hiding techniques. Discover how attackers and malicious software can abuse Microsoft Windows to hide from antivirus software and incident responders to avoid detection. Learn what indicators of compromise you can look for to give your organization a fighting chance against today's advanced attack techniques.

Mobile Malware and Spyware – Working Through the Bugs

Cindy Murphy

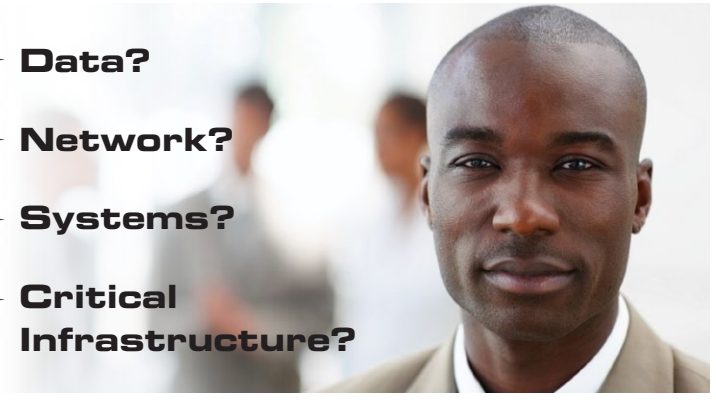
Can malware and spyware taint the evidence you find on mobile devices? Could they actually potentially help your investigation? In this session, learn the difference between malicious targeting, such as spear phishing, and inadvertent mobile malware installation from app stores and other locations. Find out what to listen for when you interview victims. Learn what to look for in mobile forensic exams, including what should trigger an in-depth malware exam. See how to unpack and decompile APK files using free tools in order to see the malware's underlying code and ascertain what it might be doing. Finally, learn what ramifications malware – or its absence – can have for your cases.

Vendor Showcase

Wednesday, July 16 | 12:00pm-1:30pm | 5:00pm-7:00pm

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.

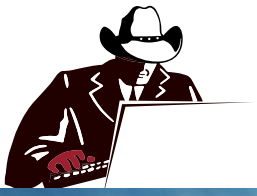
For more information, contact us at 8570@sans.org or visit www.sans.org/8570

FUTURE SANS TRAINING EVENTS

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

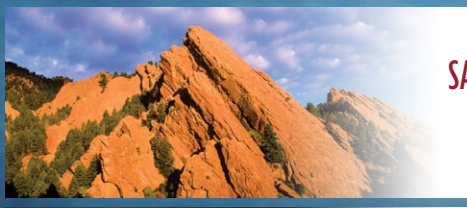
SANS Security West 2014

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 Capital City 2014

Washington, DC | July 7-12

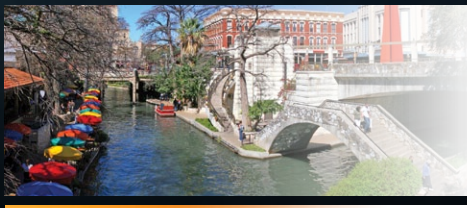
SANS ICS Industrial Control Systems

ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25

SANS Boston 2014

Boston, MA | July 28 - August 2



SANS San Antonio 2014

San Antonio, TX | August 11-16

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

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 SAN FRANCISCO 2014

Hotel Information

Training Campus

Hilton San Francisco Union Square

333 O'Farrell Street
San Francisco, CA 94102
www.sans.org/event/san-francisco-2014/location

Special Hotel Rates Available

A special discounted rate of $219.00 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 23, 2014. To make reservations, please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

As convenient as it is historic, the Hilton San Francisco Union Square hotel is one of the largest hotels on the West Coast, offering exquisite views over the city. Located in the heart of downtown San Francisco, this stylish and sophisticated hotel offers easy access to Nob Hill, Chinatown and fantastic shopping and entertainment venues in one of the USA's most diverse and dynamic cities.

Top 5 reasons to stay at the Hilton San Francisco Union Square

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 San Francisco Union Square, 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 San Francisco Union Square that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN FRANCISCO 2014

Registration Information

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

Register online at www.sans.org/event/san-francisco-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	**5/28/14**	**$400.00**	**6/11/14**	**$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