THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS

Crystal City 2014

Arlington, VA | September 8-13

Choose from these popular courses:

Mac Forensic Analysis *NEW!*

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Windows Forensic Analysis

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Mobile Device Security and Ethical Hacking

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

> *"SANS courses open your eyes to the real cyber world, and encourage thinking about security of data and network access."*
>
> -Frank Munson,
> Virginia International Terminal

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

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

We would like to invite you to **SANS Crystal City 2014** in **Arlington, Virginia** for outstanding IT security, security management, and forensic training. Join us on **September 8-13** at the **DoubleTree by Hilton Washington** for six hands-on, immersion-style security courses taught by real-world practitioners including: Dr. Eric Cole, Hal Pomeranz and Sarah Edwards, Christopher Crowley, G. Mark Hardy, Seth Misenar, and Chad Tilbury. SANS instructors meet stringent requirements for excellence, and they will ensure you will be able to apply the information you learn in class the day you get back to the office.

Threats are always changing and getting more complicated so it is vital you stay up with the times. A look at this brochure will identify ways you can boost your career and demonstrate and validate your expertise. Five courses are associated with a **GIAC** certification, three of which align with the **DoD Directive 8570**. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military and industry to protect the cyber environment. Learn which courses can help you earn your master's degree at the **SANS Technology Institute** with either a Master of Science Degree in Information Security Management (MSISM) or the Master of Science Degree in Information Security Engineering (MSISE). The SANS Technology Institute is the only accredited graduate institution focused solely on cybersecurity.

For your easy reference, also look inside for detailed course descriptions, instructor bios, and **SANS@Night** and **Special Event** evening talks. SANS evening presentations are led by instructors and are designed to enhance your training and are open to all paid attendees at no additional cost.

Our campus for this event is the **DoubleTree by Hilton Washington DC-Crystal City**. A special discount rate of $199 S/D will be honored based on space availability and high-speed Internet in your room is included. The hotel offers unparalleled panoramic views that include the Washington Monument and the Potomac River, and is just steps from trendy restaurants, Pentagon City shops, and the Pentagon City metro station – perfect for sightseeing in our nation's capital.

Register and pay by July 16 and receive a $400 tuition fee discount! Start making your training and travel plans now; let your colleagues and friends know about SANS Crystal City 2014!

SANS

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

"I now have clear objectives for evaluating our IT security program."
-Richard Reihs,
Nebraska Furniture Mart

"This course provides the foundation information needed by every IT security program."
-Paul Marchetti,
Raytheon

"I have written and read a lot of technical documentation and training since I began in IT in 1988, and this course was some of the best I have ever seen!"
-Jean Costello,
UMUC Student

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

Courses-at-a-Glance

		MON 9/8	TUE 9/9	WED 9/10	THU 9/11	FRI 9/12	SAT 9/13
SEC401	**Security Essentials Bootcamp Style**	**Page 1**					
SEC504	**Hacker Techniques, Exploits, and Incident Handling**	**Page 2**					
SEC575:	**Mobile Device Security and Ethical Hacking**	**Page 3**					
FOR408	**Windows Forensic Analysis**	**Page 4**					
FOR518	**Mac Forensic Analysis**	**Page 5**					
MGT512	**SANS Security Leadership Essentials For Managers with Knowledge Compression™**	**Page 6**					

@SANSInstitute *Join the conversation:* **#SANSCrystalCity**

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, Sept 8 - Sat, Sept 13
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Dr. Eric Cole
▸ 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.

*"Best instructor I have ever had.
Dr. Cole's energy, knowledge, and enthusiasm
make the 10-hour day bearable."*
-Tom Dempsey, Exelon Corporation

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

"Extremely useful material and I am now fired up to take follow-up courses."
-Rehan Mahmoud, Google

"Having fun while learning infosec, it doesn't get much better than that!"
-Todd Lundit, Samaritan Health

Dr. Eric Cole *SANS Faculty Fellow*

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

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Sept 8 - Sat, Sept 13
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Seth Misenar

- 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

"SEC504 is very challenging - but not in a bad way! Regardless of your experience level, you will learn something that will better you, whether it's in the workplace or at home office/network."
-Ives Bowman, DND, CFNOC

"Information security is hard. Make it easier by attending SEC504!"
-Daniel Eddy, ADM

Seth Misenar *SANS Principal Instructor*

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

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, Sept 8 - Sat, Sept 13
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley
▸ GIAC Cert: GMOB
▸ Masters Program

"SEC575 provides a pretty comprehensive overview of different attack vectors and vulnerabilities in the mobile field. It covers many topics in enough depth to really get a foothold in the subject. I wish I had taken this course several years ago when first entering the mobile landscape. It would have saved me months of painful self-teaching, and is vastly more complete in many areas."
-Jeremy Erickson, Sandia National Labs

"In the fast-paced world of BYOD and mobile device management, SEC575 is a must course for Info Sec managers."
- Jude Meche, DSCC

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **The high probability of device loss or theft, and more.**

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

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

www.giac.org

www.sans.edu

Christopher Crowley *SANS Certified Instructor*

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

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, Sept 8 - Sat, Sept 13
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Chad Tilbury
- GIAC Cert: GCFE
- Masters Program

Master Windows Forensics – What Do You Want to Uncover Today?

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

FOR408: Windows Forensic Analysis focuses on the critical digital forensics knowledge of the Microsoft Windows operating system. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation.

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

This course utilizes a brand-new Windows 8.1 based case exercise that took over 6 months to create the data. Realistic example case data takes months to create in real time correctly. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. Our development team spent months creating an incredibly realistic scenario. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The brand new case workbook, will detail the step-by-step each investigator could follow to examine the latest technologies including Windows 8.1.

Who Should Attend

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

Digital Forensics and Incident Response
digital-forensics.sans.org

www.giac.org

www.sans.edu

"Awesome coverage. FOR408 covers material in logical fashion going from 0-60 in windows forensics."

-Reed Puchron, EY

"FOR408 is a great course to get into content activities and forensics, and covers a large number of tools which is great."

-Brett Eckert, Weatherford

Chad Tilbury *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

FORENSICS 518

Mac Forensic Analysis

NEW

SANS

Six-Day Program
Mon, Sept 8 - Sat, Sept 13
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructors: Hal Pomeranz
Sarah Edwards

Digital Forensics and
Incident Response
digital-forensics.sans.org

Sarah Edwards

SANS Instructor

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counterintelligence, counter-narcotic, and counterterrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidesNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College.

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Who Should Attend

- Experienced digital forensic analysts
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Incident response team members
- Information security professionals
- FOR408, FOR508, FOR526, FOR610, FOR585 alumni looking to round out their forensic skills

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518: Mac Forensic Analysis** course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

The **FOR518: Mac Forensic Analysis Course** will teach you:

- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) file system by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- **User Activity:** How to understand and profile users through their data files and preference configurations.
- **Advanced Analysis and Correlation:** How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- **Mac Technologies:** How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

FOR518 aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

FORENSICATE DIFFERENTLY!

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the US and Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of Open Source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a Lethal Forensicator and is the creator of the SANS Linux/Unix Security course (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog. @hal_pomeranz

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS
sans.org

Five-Day Program
Mon, Sept 8 - Fri, Sept 12
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.

"G. Mark's presentation skills are fantastic! He does an incredible job of presenting a large amount of material in a limited time frame."
-Chris Shipp, DM Petroleum

"MGT512 is awesome! There is lots of material, but I will be able to go back and read the notes and study more. Very structured, relevant, and concise."
-Juan Canino, SWIFT

www.giac.org

www.sans.edu

www.sans.org/8570

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!

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.

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

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

Continuous Ownage: Why you Need Continuous Monitoring

Seth Misenar

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match.

This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course: Continuous Monitoring and Security Operations.

Automating Linux Memory Capture for Analysis *Hal Pomeranz*

Volatility has included support for Linux memory analysis since v2.2. However, practitioners have faced two obstacles: (1) Acquiring memory from a Linux system requires building, loading, and correctly using a third-party kernel module (such as LiME) for each system encountered; and (2) Creating a system-specific volatility "profile" for each system. Even for experts, these tasks are non-trivial and error-prone if performed manually. Fortunately, the Linux environment makes scripting and automation straightforward. This session presents a tool to capture actionable information from Linux systems. The tool, which has been tested and used many times, was created to be a simple, automated collection agent that can be installed on a portable USB device. The user should be able to insert the USB device into a system and execute a single command to capture the memory of the system and produce a Volatility profile for use in later analysis. This session covers the basics of Linux memory capture and Volatility profile creation as a manual process, then looks at how to install and use the tool as a portable agent. Using the Volatility framework, the session will also demonstrate some of the valuable information that can only be obtained via memory analysis.

Weaponizing Digital Currency *G. Mark Hardy*

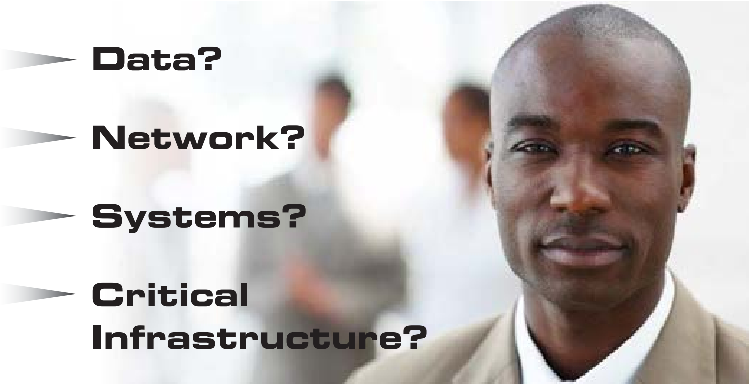
Satoshi Nakamoto wasn't stupid. In the early days, he (they) mined over 1,000,000 Bitcoins when nobody really cared. If Bitcoin continues to increase in value at the rate it did last year, someone will be holding a massive currency weapon. George Soros destabilized the British Pound in 1992 and made 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.

New School Forensics: Latest Tools and Techniques in Memory Analysis

Chad Tilbury

With memory analysis now accepted as a core component of forensics and incident response, advancements are occurring at an unprecedented pace. Notably, nearly all of the progress is taking place in free and open source tools. Whether you are just getting started with memory forensics or you have been at it since the early days, come learn about the latest and greatest additions to the memory forensics arsenal.

How Are You Protecting Your



- Data?
- Network?
- Systems?
- Critical Infrastructure?

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

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

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

MAKE YOUR NEXT MOVE COUNT
Earn a Respected Graduate Degree

"It's great to learn from an organization at the forefront of both academics, and in the field."
-Joseph Faust,
MSISE Program

Master's Degree Programs:

- ▶ M.S. in Information Security Engineering
- ▶ M.S. in Information Security Management

Specialized Graduate Certificates:

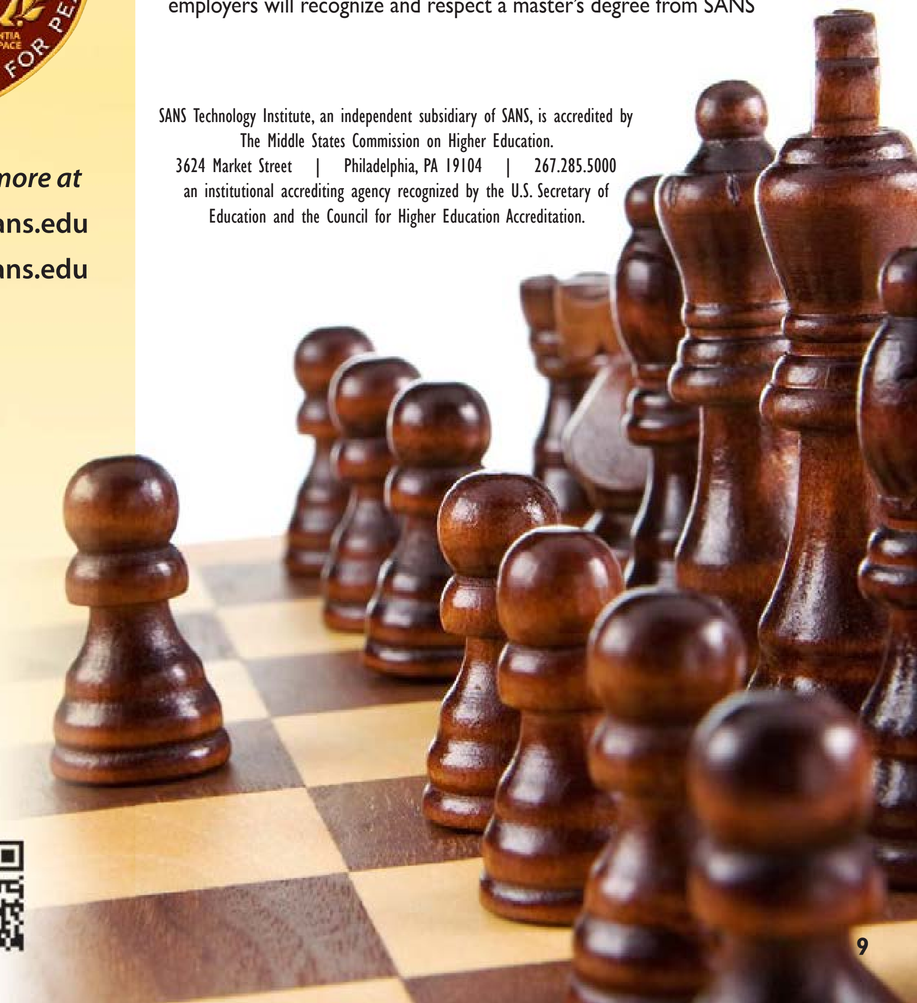
- ▶ Penetration Testing & Ethical Hacking
- ▶ Incident Response
- ▶ Cybersecurity Engineering (Core)

Top Reasons Students Choose SANS Graduate Programs:

- World-class, cutting-edge technical courses that refine and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership and who bring the material to life
- Simulation and group projects that teach students to write, present, and persuade effectively
- Validation from multiple GIAC certifications even before you earn your degree
- Flexibility to attend courses when and where you need them, either live in classrooms or online from home or work
- A reputation that helps accelerate career growth—employers will recognize and respect a master's degree from SANS

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

Learn more at
www.sans.edu
info@sans.edu



SECURING THE HUMAN

SECURITY AWARENESS FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.

- Create your own training program by choosing from a variety of modules:

  - STH.End User is mapped against the Critical Security Controls.

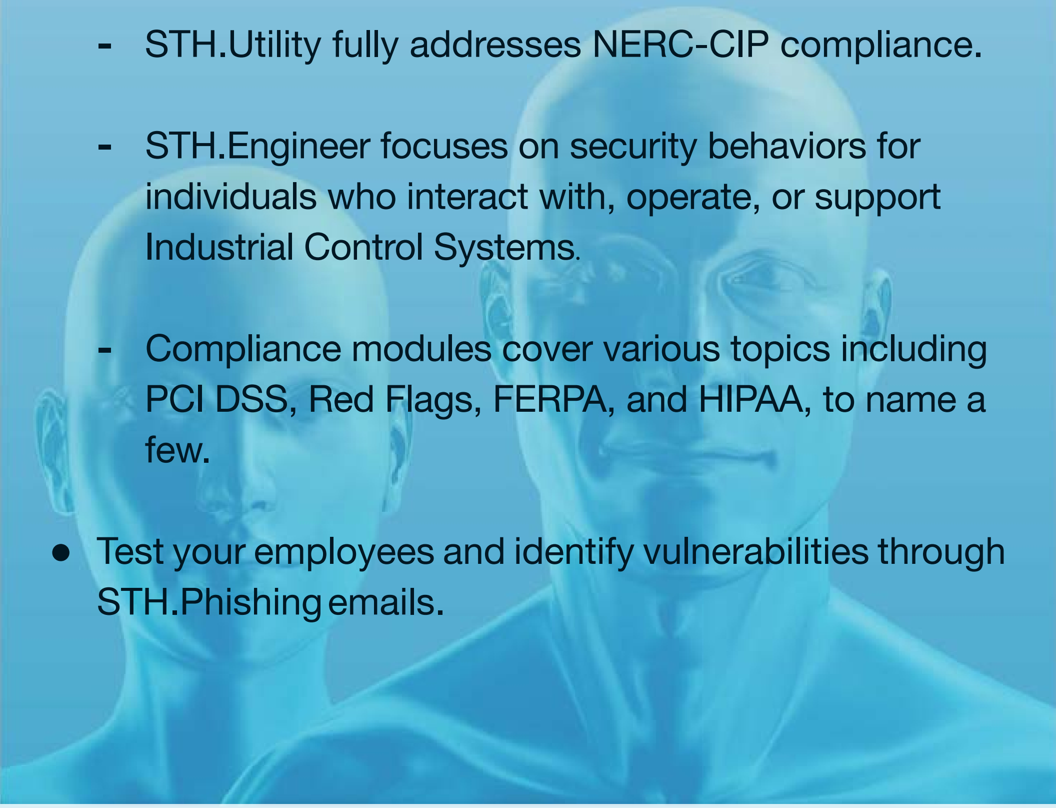
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.

  - STH.Utility fully addresses NERC-CIP compliance.

  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.

  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.

- Test your employees and identify vulnerabilities through STH.Phishing emails.



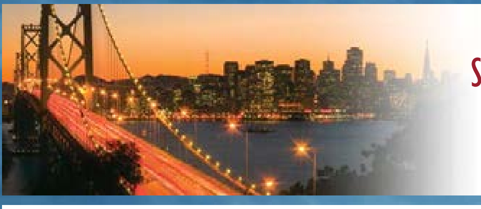
For a free trial visit us at:
www.securingthehuman.org

FUTURE SANS TRAINING EVENTS

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

SANS Capital City 2014

Washington, DC | July 7-12



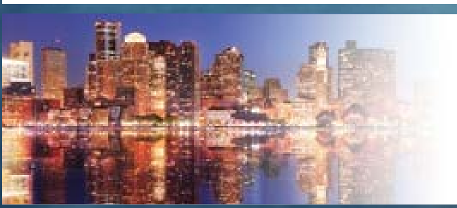
SANS San Francisco 2014

San Francisco, CA | July 14-19

SANS Industrial Control Systems

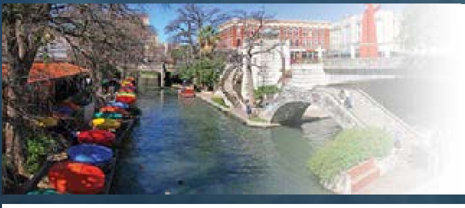
ICS Security TRAINING 2014 - HOUSTON

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 Cyber Defense SUMMIT

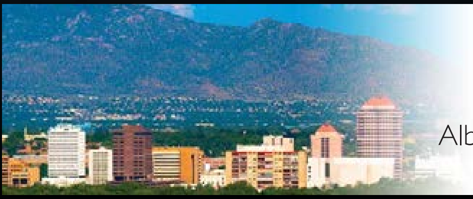
Nashville, TN | August 13-20

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

SANS Chicago 2014

Chicago, IL | August 24-29



SANS Albuquerque 2014

Albuquerque, NM | September 15-20

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 CRYSTAL CITY 2014

Hotel Information

Training Campus

DoubleTree by Hilton Washington DC-Crystal City

300 Army Navy Drive | Arlington, VA 22202
www.sans.org/event/crystal-city-2014/location

Special Hotel Rates Available

A special discounted rate of $199.00 S/D will be honored based on space availability. This rate is lower than the current Government per diem rate. These rates include high-speed Internet in your room and are only available through August 17, 2014.

Expect stunning US capital views from the DoubleTree by Hilton Hotel Washington DC-Crystal City. Located in Arlington, Virginia, the hotel offers unparalleled panoramic views that include the Washington Monument and the Potomac River. The hotel is just steps from trendy restaurants, Pentagon City shops, and only three blocks to the Pentagon City metro station – perfect for sightseeing in our nation's capital.

Top 5 reasons to stay at the Doubletree Hotel Crystal City

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 Doubletree Hotel Crystal City, 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 Doubletree Hotel Crystal City that you won't want to miss!

5 Everything is in one convenient location!

SANS CRYSTAL 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/crystal-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	7/16/14	$400.00	7/30/14	$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 August 20, 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