THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Seattle 2014

Seattle, WA Sept 29 - Oct 6

Choose from these popular courses:

Mac Forensic Analysis ***NEW!***

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Windows Forensic Analysis

Mobile Device Security and Ethical Hacking

IT Security Strategic Planning, Policy and Leadership

Metasploit Kung Fu for Enterprise Pen Testing

"SANS courses are always the best six days of the year!"

-Erich Knaak,
School Employees
CU of Washington

GIAC Approved Training

Register at sans.org/event/seattle-2014

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

We are excited to invite you to attend the **SANS Seattle 2014** training event from **September 29-October 6**. Cyber attacks against devices and systems are on the increase, so protecting your data is critical. The lineup of hands-on courses in IT security, forensics, and security management and leadership at SANS Seattle 2014 will provide you with the most up-to-date security information to address today's cyber threats.

A look through the SANS Seattle 2014 brochure lays out in detail each of the courses offered and the instructors, including Dr. Eric Cole, Stephen Northcutt, Hal Pomeranz, Dave Shackleford, Christopher Crowley, Mike Pilkington, Sarah Edwards, and Mark Williams. These top experts in the field will ensure that you can use what you learn the minute you get back to your office.

The **GIAC** certification page in this brochure provides you with information on how to get certified and join more than 58,000 other certification holders recognized as experts in the IT industry. It also indicates which certification requirements are approved for the **DoD Directive 8570**.

Are you looking to earn your master's degree in cybersecurity? You can take courses in **Information Security Management** (MSISM) or **Engineering** (MSISE) at the SANS Technology Institute, the only accredited graduate institution focused solely on cybersecurity. The **SANS Technology Institute** also offers specialized graduate certificates.

At SANS Seattle 2014, you can combine your cybersecurity training with visits to Seattle's renowned museums: Art, Aviation and Transpiration, History and Heritage, and Science and Nature. Or you can explore the grandeur of the Pacific Northwest with an outdoor day trip to Mount Rainier, Bainbridge Island, Snoqualmie Falls, or the Olympic Peninsula.

Our campus for SANS Seattle 2014, the **Renaissance Seattle Hotel**, is located in the heart of downtown and features stunning views of Puget Sound, the mountains, and the city skyline. The hotel is just minutes away from CenturyLink and Safeco Fields, Pike Place Market, and upscale shopping. It is also convenient to the Sea-Tac airport and has easy access to major freeways.

A special discounted rate of $175.00 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 August 29, 2014.

Register and pay by August 13, 2014 to save up to $400 on tuition fees! Let your colleagues and friends know about SANS Seattle 2014 and start making your training and travel plans now. We look forward to seeing you in Seattle!

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

"The knowledge I am gaining is giving me excellent insight as to how to protect my environment!"
-Jon Louie, Eagle County Government, Colorado

"It's a good sign if you come into the course concerned about the material and leave confident at the end of the lesson."
-David Fawley, ANSYS, Inc.

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

Courses-at-a-Glance

		MON 9/29	TUE 9/30	WED 10/1	THU 10/2	FRI 10/3	SAT 10/4	SUN 10/5	MON 10/6
SEC401	Security Essentials Bootcamp Style	Page 1							
SEC504	Hacker Techniques, Exploits & Incident Handling	Page 2							
SEC575	Mobile Device Security and Ethical Hacking	Page 3							
SEC580	Metasploit Kung Fu for Enterprise Pen Testing							Pg 4	
FOR408	Windows Forensic Analysis	Page 5							
FOR518	Mac Forensic Analysis	Page 6							
MGT514	IT Security Strategic Planning, Policy & Leadership	Page 7							

@SANSInstitute *Join the conversation:* #SANSSeattle

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Sept 29 - Sat, Oct 4
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.

Who Should Attend

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

"Eric is incredible; he never ceases to amaze me with his ability to relate the information to everyone while keeping the material interesting."

-Brian Ward, Jackson Supply

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.

"Dr. Cole is an excellent instructor who makes the material very easy to understand and guaranteed to stick."
-Garrett Krutilla, First Energy

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

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

SANS

Six-Day Program
Mon, Sept 29 - Sat, Oct 4
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Dave Shackleford

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

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

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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

"SEC504 was excellent and showed incident handlers the other side of how hackers are getting into the system we are defending."
- Jacob Patterson, USFK J6

"It's great to understand how hackers are exploiting a variety of systems. Learning how to prevent these as best as possible is imperative to protect key systems and resources. SEC504 course concepts are great!."
-Samantha Hanagan, Texel Tek

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. @daveshackleford

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, Sept 29 - Sat, Oct 4
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley
- GIAC Cert: GMOB
- Masters Program

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.

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

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

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

"BYOD provides numerous attack vectors. SEC575 identifies procedures to protect and identify pathways that need to be corrected."
-Russ Hall, Northrop Grumman

"Chris is an impressive instructor. He speaks to all levels, provides excellent examples, and knows his stuff!"
-Jon Louie, Eagle Co. Gov't

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

SECURITY 580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Program
Sun, Oct 5 - Mon, Oct 6
9:00am - 5:00pm
12 CPE/CMU Credits
Laptop Required
Instructor:
Christopher Crowley

SANS Brochure Challenge

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit, are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an Open Source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

Who Should Attend

- This class would be essential to any industry that has to test regularly as part of compliance requirements or regularly tests their security infrastructure as part of healthy security practices.
- Penetration testers
- Vulnerability assessment personnel
- Auditors
- General security engineers
- Security researchers

"I appreciate the 'amateur vs. above average' and the focus on how to be excellent. I am a professional and new to this business so these kinds of insights from high-quality pros make a difference."

-Michael Decker, CNS Security

"SEC580 is well thought out course material that takes you step-by-step through the meat and potatoes of metasploit."

-Scott Tirapelle, Franchise Tax Board

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 29 - Sat, Oct 4
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Pilkington
- GIAC Cert: GCFE
- Masters Program

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

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.

Who Should Attend

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

FOR408: Windows Forensic Analysis focuses on 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.

giac.org

sans.edu

"In my 12 years of professional experience, FOR408 has been the best training I've had."
-Rafael Cruz, Mercantil CB

"Mike was amazing. His knowledge and helpful attitude made it a great week. I look forward to taking a class from him again in the future."
-Matt Edmondson, DHS

Mike Pilkington *SANS Instructor*

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

FORENSICS 518

Mac Forensic Analysis

NEW

SANS

Six-Day Program
Mon, Sept 29 - Sat, Oct 4
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructors: Hal Pomeranz
Sarah Edwards

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

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

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!

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.

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 514

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, Sept 29 - Fri, Oct 3
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Recommended
Instructors: Stephen Northcutt
Mark Williams

- Masters Program

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but we almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack.

Who Should Attend

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

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

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

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.

www.sans.edu

Mark Williams

SANS Instructor

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

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. @StephenNorthcutt

SEATTLE 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.

The State of Eavesdropping on Cellular Networks *Christopher Crowley*

Security research in the 3G and 4G network space is restricted due to legal issues in the United States. Christopher Crowley will discuss the current known, open source information related to known cellular attacks. He will also discuss the attack methodology associated with cellular client duping, a strategy for convincing a cellular device to connect to an attacker controlled cell tower.

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

In most enterprise networks, there are a number of privileged accounts that are used for maintaining the Windows domain, including accounts for domain administration, configuration management, patch management, vulnerability analysis, and of course incident response. In all of these cases, the accounts have the ability to logon to most, if not all, Windows hosts in the environment. These accounts therefore become high-value targets for attackers. In order to protect these privileged domain accounts, it is important to have a solid understanding of the various circumstances that can expose domain account credentials. In this presentation, I will discuss what you can and cannot do safely with domain accounts. In particular, I will cover attacks against password hashes, security support providers, access tokens, and network authentication protocols. I will then provide a set of recommendations that you can follow to mitigate the risks and protect those privileged domain account credentials in your environment.

Investing for Retirement *Stephen Northcutt*

When I turned 50, I joined AARP so I could get 20% off Regal Theaters popcorn and other swell discounts, but it seemed that every single issue of their magazine had an article on people not saving enough to retire. However, saving for retirement is silly, the best interest rate I have seen on a savings account is 0.7% and that is probably less than the true cost of living increases. If any of us are going to retire, we will need to invest and invest wisely. Since I am older than most of the SANS instructors, it occurred to me that I would probably be one of the first to go. For the last year, I have been looking at the options to generate enough monthly income to retire on and have found the results rather surprising. This talk summarizes my research, it will cover many of the financial vehicles that are available and for each we will cover the pitch, the catch, and my best assessment on how to use (or avoid) that vehicle. The talk is meant to encourage each member of the audience to begin thinking about their financial portfolio and retirement options. Best of all, I promise I will not try to sell anybody anything.

Vendor Showcase

Wednesday, October 1 | 10:30-10:50am | 12:00-1:30pm | 3:00-3:20pm

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.

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:

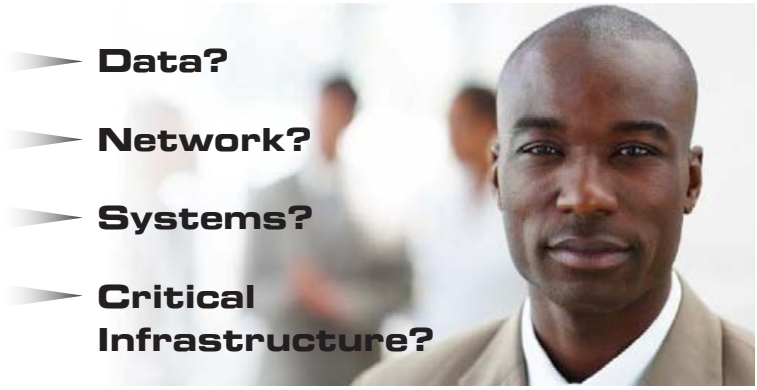
- World-class, cutting-edge technical courses that refine and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership and who bring the material to life
- Simulation and group projects that teach students to write, present, and persuade effectively
- Validation 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
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

Learn more at
sans.edu
info@sans.edu

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.

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

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

Global Information Assurance Certification GIAC www.giac.org

Get Certified at **giac.org**

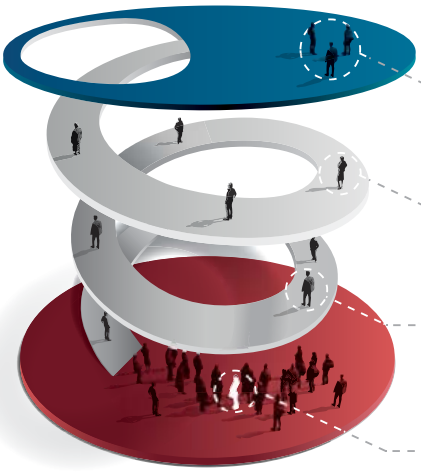
SANS CyberTalent Powered by GIAC

Contact Us to Learn More

sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

Introducing SANS CyberTalent Assessments, a new web-based recruitment and talent management tool that helps validate the skills of information security professionals. This unique tool may be used during the recruitment process of new information security employees and to assess the skills of your current staff to create a professional development plan. This tool will save you money and time, as well as provide you with the information required to ensure you have the right skills on your information security team.



Benefits of SANS CyberTalent Assessments

For Recruiting

- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

For Talent Management

- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps develop a professional development plan

US and Canada 301.654.SANS (7267) EMEA and APAC inquiries: + 44 (0) 20 3598 2363

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

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 computer based training modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - 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.

SANS SECURING THE HUMAN

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

FUTURE SANS TRAINING EVENTS

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

SANS Boston 2014

Boston, MA | July 28 - August 2

SANS San Antonio 2014

San Antonio, TX | August 11-16

Cyber Defense
SUMMIT & TRAINING

Nashville, TN | August 13-20

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

SANS Chicago 2014

Chicago, IL | August 24-29

SANS Crystal City 2014

Crystal City, VA | September 8-13

Retail Cyber Security
SUMMIT & TRAINING

Dallas, TX | September 8-17

Security Awareness
SUMMIT & TRAINING

Dallas, TX | September 8-17

SANS Albuquerque 2014

Albuquerque, NM | September 15-20

SANS SEATTLE 2014

Hotel Information

Training Campus
Renaissance Seattle Hotel

515 Madison Street
Seattle, WA 98104
sans.org/event/seattle-2014/location

Escape to the Renaissance Seattle Hotel, a stylish hotel in Seattle conveniently located just minutes from Pike Place Market and upscale shopping. There is always something wonderfully new to discover while staying at this hotel. Unwind in spacious guest rooms with stunning views of Puget Sound, the mountains and city skyline. Enjoy casual dining coupled with spectacular city views at R View, a premier Seattle hotel restaurant. Come discover how this hotel seamlessly combines luxury, comfort and technology into an unforgettable urban retreat.

Special Hotel Rates Available

A special discounted rate of $175.00 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 August 29, 2014.

Top 5 reasons to stay at the Renaissance Seattle Hotel

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 Renaissance Seattle Hotel, 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 Renaissance Seattle Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS SEATTLE 2014

Registration Information

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

Register online at sans.org/event/seattle-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	**8/13/14**	**$400.00**	**8/27/14**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by September 10, 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.
sans.org/vouchers