THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Chicago 2013

Chicago, IL | October 28 - November 2

SANS hands-on infosec training comes to Chicago!

Featuring these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Computer Forensic Investigations – Windows In-Depth

SANS +S Training Program for the CISSP® Certification Exam

Auditing Networks, Perimeters, and Systems

Mobile Device Security and Ethical Hacking

IT Project Management, Effective Communication, and PMP® Exam Prep

"SANS is by far the best hands-on training. The instructors are very knowledgeable and know how to transfer that to students."

-Rob Brabers, Sincerus

GIAC Approved Training

Register at www.sans.org/event/chicago-2013

Save $500 by registering early!

See page 13 for more details.

Dear Colleagues,

What happens when best-in-class security training is offered in a world-class city? A great experience! I can attest to both, working at SANS and living in Chicago for 12 years. Make your reservation early to capitalize on cost savings and come join us for six days of intensive, hands-on training at the spacious **Palmer House Hotel** located in the heart of Chicago's loop October 28th - November 2nd. **Register and pay by September 11, 2013 and save up to $500 on tuition fees with discounts offered to early registrants.**

Dennis Scandrett

What makes a great event? Great courses and great instructors! We are bringing seven of the brightest minds in the industry to teach seven of SANS' most popular six-day courses including *SEC575: Mobile Device Security and Ethical Hacking* and *MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep*. Taught by our top instructors, this event offers an intimate opportunity to learn, network, and practice the hands-on skills that will boost your career. Learn from James Tarala, Paul A. Henry, Jeff Frisk, Christopher Crowley, Seth Misenar, Jonathan Ham, and Mike Pilkington. Our instructors will ensure that what you learn in the classroom, you will be able to use immediately upon returning to the office the SANS promise in action.

See the brochure for course descriptions and instructor bios. Be sure to sign up for your *GIAC Certification* at bundled, reduced rates. This brochure will also tell you about which SANS courses align with the *DoD 8570 Directive*. Another thing to look for is how to earn your master's degree through *SANS Technology Institute (STI)*. Take classes in Information Security Management (MSISM) or Engineering (MSISE). You can pick a course that will contribute to all of these options that are important to you!

For the third year, our campus is the Palmer House Hilton Hotel. The past year's attendees have enjoyed this wonderful 140-year-old hotel that has undergone renovations to enhance the spectacular décor. See page 13 for details on how to get the best savings. You will have easy access to Lake Michigan, Millennium Park, and Grant Park where you can see incredible sculpture and gardens. You are close to the Art Institute of Chicago and Macy's on State Street; and you are just blocks from the Magnificent Mile, Water Tower Place, The Shops of Northbridge, and The 900 Shops. Of course there is much, much more with the following attractions also being close to the hotel: Shedd Aquarium, Adler Planetarium and Field Museum, and all the great dining, theater, symphony, and opera that comes with a major US city. Travelers to this city find that downtown Chicago is friendly and clean; and people that you meet want you to share their love of their city!

Enhance your training by attending our evening talks, complimentary for registered SANS Chicago 2013 students! So let your colleagues and friends know about SANS Chicago 2013. If you can't attend, please pass this brochure to any interested colleagues. We look forward to seeing you in Chicago!

Dennis Scandrett

Director of Audit and General Security Curricula

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

"Excellent training! Instructors are passionate and enthusiastic. I look forward to the classes."
-Bernardine Krupka, US Bank

"I never thought I could learn so much in such short time without feeling burned out. Great job making it engaging and interesting."
-Jeff Eubanks, Mainstream Engineering Corp.

"I'm a repeat student at SANS conference. Always great courses and knowledgeable instructors."
-Linh Sithihao, Health Care

Courses-at-a-Glance

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Paul A. Henry

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 not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. 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 and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore we will teach you how 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.

Who Should Attend:

- **Security professionals who want to fill the gaps in their understanding of technical information security**
- **Managers who want to understand information security beyond simple terminology and concepts**
- **Operations personnel who do not have security as their primary job function but need an understanding of security to be effective**
- **IT engineers and supervisors who need to know how to build a defensible network against attacks**
- **Administrators responsible for building and maintaining systems that are being targeted by attackers**
- **Forensic, penetration testers, auditors who need a solid foundation of security principles so they can be effective as possible at their jobs**
- **Anyone new to information security with some background in information systems and networking**

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in cyber security. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of 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. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

DoDD 8570 Required
www.sans.org/8570

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the *Information Security Management Handbook*, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
Laptop Required • 37 CPE/CMU Credits
Instructor: Jonathan Ham

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, 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.

"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."
-Joshua Anthony, West Virginia Army National Guard

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."
-Anthony Liu, Scotia Bank

"Fantastic class! Fantastic Instructor! I have taken six SANS classes, I have not had a bad experience yet, they are just so professionally done!"
-Rafael Cabrera, Air Force

Jonathan Ham *SANS Certified Instructor*

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

DoDD 8570 Required
www.sans.org/8570

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Christopher Crowley

Now updated to cover Apple iOS 6, BlackBerry 10, Android Jelly Bean, and Windows Phone 8

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 by 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 enterprise resource planning 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:

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

The security risks of mobile phone and tablet device use in the workplace

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.

"With the mad rush towards mobile device adoption at the point of sale and industry regulations and laws struggling to keep up, thank goodness SANS helps companies maintain secure operations."
-Dean Altman, Discount Tire

From mobile device security policy development, to design and deployment, and more

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 from 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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

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, 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.

www.giac.org

www.sans.edu

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Pilkington

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threats, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and calling in cybercrime law enforcement agents to piece together what happened in these cases.

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

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

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008) you will be exposed to well known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that students can take with them.

"Hands down the BEST forensics class EVER!! Blew my mind at least once a day for 6 days!"
-Jason Jones, USAF

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

What you will receive with this course

- **Windows version of the SIFT Workstation Virtual Machine**
- **Windows 8 Standard Full Version License and Key for the Windows SIFT Workstation**
- **Full License to AccessData FTK and Guidance Software EnCase for a 3 month trial**
- **Full License to MagnetForensics Internet Evidence Finder for a 15 day trial**
- **Two full real-world cases to examine during class**
- **Course DVD loaded with case examples, tools, and documentation**
- **Wiebetech Ultradock v5 Write Blocker Kit**

DFIR
http://computer-forensics.sans.org

"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."
-Alexander Applegate, Auburn University

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.

www.giac.org

"The best part of this class is the step-by-step process on how to use the tools and screen shots of each step. The description of each of the tools, artifacts, and analysis is the best I've ever seen."
-Rebecca Passmore, FBI

www.sans.edu

MANAGEMENT 414

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

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Seth Misenar

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

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

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

Obtaining your CISSP® certification consists of:

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

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

"This course breaks down the huge CISSP study books into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent."
-Jeff Jones, Constellation Energy Group

"This class focuses like a laser on the key concepts you'll need to understand the CISSP exam. Don't struggle with thousand page textbooks – let this course be your guide!"
-Carl Williams, Harris Corporation

Who Should Attend:

- **Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)²**
- **Managers who want to understand the critical areas of network security**
- **System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains**
- **Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job**

Take advantage of SANS CISSP® Get Certified Program currently being offered.
www.sans.org/special/cissp-get-certified-program

Seth Misenar *SANS Certified Instructor*

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including SEC401: SANS Security Essentials Bootcamp Style, SEC504: Hacker Techniques, Exploits, and Incident Handling, and SEC542: Web App Penetration Testing and Ethical Hacking. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

www.giac.org

DoDD 8570 Required
www.sans.org/8570

MANAGEMENT 525

IT Project Management, Effective Communication, and PMP® Exam Prep

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jeff Frisk

Who Should Attend:

- Individuals interested in preparing for the Project Management Professional (PMP®) Exam
- Security professionals who are interested in understanding the concepts of IT project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk sensitive projects and applications
- Anyone who would like to utilize effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/design position who works regularly with project management staff

With updated course contents to help you prepare for the updated 2013 PMP® Exam, **MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep** is a PMI Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. This course has been recently updated to fully prepare you for the updated 2013 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide* (Fifth Edition) and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management – from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide* is provided to all participants. You can reference the *PMBOK® Guide* and use your course material along with the knowledge you gain in class to prepare for the Project Management Professional (PMP®) Exam and the GIAC Certified Project Manager Exam.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

"Within the first five minutes I knew this would be a very different (and welcomed) experience than prior training with other vendors. SANS' attention to detail is evident in every slide."
-Jayme Jordan, Raytheon

Jeff Frisk *SANS Certified Instructor*

Jeff Frisk currently serves as the director of the GIAC certification program and is a member of the STI Curriculum Committee. Jeff holds the PMP certification from the Project Management Institute and GIAC GSEC credentials. He also is a certified SANS instructor and course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from The Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

www.giac.org

www.sans.edu

AUDIT 507

Auditing Networks, Perimeters, and Systems

Six-Day Program • Mon, Oct 28 – Sat, Nov 2
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

Who Should Attend:

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

"By far, this is the most hands-on, technical tool-oriented auditing class I have ever seen. I cannot imagine another class that forces you to use real tools in real situations. It is just like gaining real world experience."

-Jay Russell, U.S. Navy

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and experience the mix of theoretical, hands-on, and practical knowledge.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/chicago-2013.

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

www.giac.org

www.sans.edu

DoDD 8570 Required
www.sans.org/8570

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: Cloud IR & Forensics *Paul A. Henry*

The move to private and public cloud changes many things including how we respond for IR and forensics. As an example: traditionally in a physical realm we relied upon imaging a server's hard drive as well as RAM to perform a thorough analysis. Today in the cloud, creating a forensically sound image of an "instance" of a server to capture the server's abstracted hard disk and an image of its RAM brings new technical and legal complications. An additional issue to consider is that some vendor's platforms are simply not fully supported by our current IR & forensics tools; today's commercial tools lack the ability to perform any analysis at all on a VMware VMFS file system. Lastly, downloading a large server image may simply be cost prohibitive due to the high bandwidth costs associated with moving data out of the cloud environment.

The best course of action may be to perform your analysis within the cloud - however, the methods used in the analysis within the cloud must be forensically sound and as always in computer forensics, they must be repeatable and the result must be the same findings. In this session we will begin to explore the changes that simply must be made to your IR and forensics procedures to properly address IR & forensics in the cloud.

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.made to your IR and forensics procedures to properly address IR & forensics in the cloud.

An Introduction to PowerShell for Security Assessments *James Tarala*

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone all in with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of the Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

SANS 8 Mobile Device Security Steps *Chris Crowley*

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

Introducing the CompTIA® CASP™ Exam *Seth Misenar*

Seth Misenar, coauthor of *Syngress CISSP® Study Guide* (written with Eric Conrad), will introduce you to the new CompTIA® Advanced Security Practitioner certification, a hands-on technical exam with a mix of deeper technical questions, as well as higher-level management questions. The CASP™ was recently added to DoD 8570 for the following roles: IAT level III, IAM II, and IASAE level I and II. Come find out where CASP fits into the security certification landscape and see if Eric and Seth's new SANS prep course for the CASP is right for you.

Vendor Showcase

Monday, October 28 | 10:30am-10:50am • 12:30pm-1:15pm • 3:00pm-3:20pm

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

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

The SANS Technology Institute (STI) offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

"A degree is great. A graduate degree plus current actionable knowledge is even better. STI provides this and more."
-Seth Misenar, MSISE Student

Apply today!
Cohorts are forming now.

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE

www.sans.edu
info@sans.edu
720.941.4932

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 20 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

SANS
CYBER GUARDIAN
PROGRAM

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Real Threats
Real Skills
Real Success

Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above) or CISSP certification

Core Courses

SEC503 (GCIA) | SEC504 (GCIH) | SEC560 (GPEN) | FOR508 (GCFA)

After completing the core courses, students must choose one course and certification from either the Blue or Red Team

Blue Team Courses

SEC502 (GCFW) | SEC505 (GCWN) | SEC506 (GCUX)

Red Team Courses

SEC542 (GWAPT) | SEC617 (GAWN) | SEC660 (GXPN)

Join Today!

Contact us at **onsite@sans.org** to get started!

www.sans.org/cyber-guardian

SECURITY AWARENESS
FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPPA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org

Future SANS Training Events

SANS **Capital City** 2013

Washington, DC | September 3-8

www.sans.org/event/sans-capital-city-2013

SANS **Network Security** 2013

Las Vegas, NV | September 14-23

www.sans.org/event/network-security-2013

SANS **Seattle** 2013

Seattle, WA | October 7-14

www.sans.org/event/seattle-2013

SANS **Baltimore** 2013

Baltimore, MD | October 14-19

www.sans.org/event/baltimore-2013

SANS **South Florida** 2013

Fort Lauderdale, FL | November 4-9

www.sans.org/event/sans-south-florida-2013

SANS **Pen Test Hackfest**
TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

www.sans.org/event/pen-test-hack-fest-2013

SANS **San Diego** 2013

San Diego, CA | November 18-23

www.sans.org/event/san-diego-2013

SANS **San Antonio** 2013

San Antonio, TX | December 3-8

www.sans.org/event/san-antonio-2013

SANS Training Formats

LIVE CLASSROM 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
Convenient online instruction from SANS' top instructors
www.sans.org/vlive

Simulcast
Attend a SANS training event without leaving home
www.sans.org/simulcast

CyberCon
Live online training event
www.sans.org/cybercon

SelfStudy
Self-paced online training for the motivated and disciplined infosec student www.sans.org/selfstudy

SANS Chicago 2013

Hotel Information

Training Campus
Palmer House Hilton Hotel

17 East Monroe Street
Chicago, IL 60603
www.sans.org/event/chicago-2013/location

Special Hotel Rates Available

A special discounted rate of $219.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through October 4, 2013. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

140 Years. Countless Stories. The Palmer House didn't become a beloved downtown Chicago hotel by chance. It did so by design. Since 1871, the iconic Chicago hotel has been host to countless celebrated figures. Today, having undergone a meticulous $170 million renovation, the Palmer House awaits those stories yet to be written and forever to be retold. We invite you to share in the inspired story of this downtown Chicago hotel. Even more so, within the walls and halls of the Palmer House, we encourage you to compose your own.

Top 5 reasons to stay at the Palmer House Hilton 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 Palmer House Hilton 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 Palmer House Hilton Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS Chicago 2013

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/chicago-2013

To register, go to
www.sans.org/event/chicago-2013

Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course:
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.

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at 301-654-7267 9am - 8pm ET.

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 October 2, 2013 – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	9/11/13	$500.00	9/25/13	$250.00

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 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.

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