SANS Chicago 2012

October 27 - November 5, 2012

The Most Trusted Source for Information and Software Security Training

Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Network Penetration Testing and Ethical Hacking

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Securing Windows and Resisting Malware

Advanced Computer Forensic Analysis and Incident Response

Virtualization and Private Cloud Security

Advanced Web App Penetration Testing and Ethical Hacking

"Amazing amount of material, made comprehensible and easy to absorb in a short time!"

-Erick McCroskey, Institute of Defense Analyses

Register at
www.sans.org/chicago-2012

GIAC Approved Training

Dear Colleague,

I am pleased to invite you to our downtown Palmer House campus for **SANS Chicago 2012**, October 27-November 5. We're bringing you seven of our most popular 5- and 6-day courses, including our new cutting-edge Security 579: Virtualization and Private Cloud Security, Security 642: Advanced Web App Penetration Testing and Ethical Hacking, and Forensics 508: Advanced Computer Forensic Analysis and Incident Response. **Register by September 12 to receive a $500 tuition fee discount!**

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 Dr. Eric Cole, Jason Fossen, Paul A. Henry, Kevin Johnson, Lance Spitzner, Chris Brenton, and me.

See the brochure for course descriptions and instructor bios. Be sure to sign up for your *GIAC Certification* at bundled, reduced rates. Another thing to look for is how to earn your Master's Degree from the SANS Technology Institute (STI). Learn more about STI at **www.sans.edu**.

For the second year our campus is **The Palmer House Hilton Hotel**. Last year's attendees enjoyed this wonderful 140-year-old hotel that has undergone renovations to enhance the spectacular décor. See the hotel page in the brochure for details on how to get the best savings. A downtown hotel means you have easy access to Lake Michigan, Millennium Park, and Grant Park where you can see incredible sculpture and gardens. You are a block from Lake Michigan in all its grandeur. 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, clean, and safe; and people that you meet want you to share their love of their city!

So let your colleagues and friends know about SANS Chicago 2012. If you can't attend, please pass this brochure to any interested colleagues. We look forward to seeing you in Chicago!

Best regards,

Stephen Northcutt
President, SANS Technology Institute

Stephen Northcutt

Here is what past attendees had to say about their SANS training experience:

"Got SANS? SANS always is one of the first places I look for information. Not only because of the quantity - - but also the quality."
-Bill Coffey, Shaw AFB

"I've been to three previous SANS events, they are always well done and most impressive; they are always valuable."
-Charles Higgins, Northwest Hospital Corp.

"SANS courses and instructors are the best I have ever experienced.
-Diane Matt, Department of National Defense

Courses-at-a-Glance

		SAT 10/27	SUN 10/28	MON 10/29	TUE 10/30	WED 10/31	THU 11/1	FRI 11/2	SAT 11/3	SUN 11/4	MON 11/5
SEC401	SANS Security Essentials Bootcamp Style			PAGE 1							
SEC505	Securing Windows and Resisting Malware			PAGE 2							
SEC560	Network Penetration Testing & Ethical Hacking			PAGE 3							
SEC579	Virtualization and Private Cloud Security			PAGE 4							
SEC642	Advanced Web App Penetration Testing and Ethical Hacking			PAGE 5							
FOR508	Advanced Computer Forensic Analysis and Incident Response			PAGE 6							
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™			PAGE 7							
MGT433	Securing The Human: Building and Deploying an Effective Security Awareness Program	PG 8									
SEC542	Cloud Security Fundamentals									PG 8	

Security 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, Oct 29 - Sat, Nov 3
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance 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 up-to-the-minute 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. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

SPECIAL NOTE: This course is endorsed by the Committee on National Security Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).

Test your security knowledge with our SANS Security Essentials Assessment Test. Get your free test at **www.sans.org/assessments**

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**
- **Anyone new to information security with some background in information systems and networking**

Bootcamp

This program has extended hours.
Security 401 PARTICIPANTS ONLY
Evening Bootcamp Sessions:
5:15pm - 7:00pm (Days 1-5)

Attendance is required for the evening bootcamp sessions as the information presented appears on the GIAC exams. These daily bootcamps give you the opportunity to apply the knowledge gained throughout the course in an instructor-led environment. It helps fill your toolbox with valuable tools you can use to solve problems when you go back to work. The material covered is based on Dr. Eric Cole's "Cookbook for Geeks," and most students find it to be one of the highlights of their Security Essentials experience! Students will have the opportunity to install, configure, and use the tools and techniques they have learned. CDs containing the software required will be provided for each student. Students should arrive with a laptop properly configured. A working knowledge of each operating system is recommended but not required. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

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. Dr. Cole 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 in which 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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 505

Securing Windows and Resisting Malware

Six-Day Program • Mon, Oct 29 - Sat, Nov 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Fossen

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The Securing Windows and Resisting Malware course is fully updated for Windows Server 2012, Windows 8, Server 2008-R2, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact on users of these changes. You'll see the instructor demo the important steps live, and, you can use your laptop to follow along. The manuals are filled with screenshots and step-by-step exercises, so you can do the steps alongside the instructor in seminar or later on your own time if you prefer.

We've all got anti-virus scanners, but what else needs to be done to combat malware and intruders using Advanced Persistent Threat (APT) techniques? Today's weapon of choice for hackers is stealthy malware with remote control channels, preferably with autonomous worm capabilities, installed through client-side exploits. While other courses focus on detection or remediation, the goal of this course is to prevent the infection in the first place (after all, first things first).

Especially in Server 2012 and beyond, PowerShell dominates Windows scripting and automation. It seems everything can be managed through PowerShell now. And if there's a needed skill that will most benefit the career of a Windows specialist, it's being able to write PowerShell scripts because most of your competition will lack scripting skills, so it's a great way to make your resume stand out. This course devotes an entire day to PowerShell scripting, but you don't need any prior scripting experience.

This course will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows expertise.

You are encouraged to bring a virtual machine running Windows Server 2012 Standard or Datacenter Edition configured as a domain controller, but this is not a requirement for attendance since the instructor will demo everything discussed on-screen. You can get a free evaluation version of Server 2012 from Microsoft's web site (just do a search on "site:microsoft.com Server 2012 evaluation trial"). You can use Hyper-V, VMware, VirtualBox, or any other virtual machine software you wish.

This is a fun course and a real eye-opener even for Windows administrators with years of experience. Get the PowerShell scripts now for the course from **www.sans.org/windows-security** (go to the Downloads link). There is no prior registration required, and all scripts are in the public domain.

Who Should Attend:

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the SANS Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- IIS administrators and webmasters with servers at risk

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

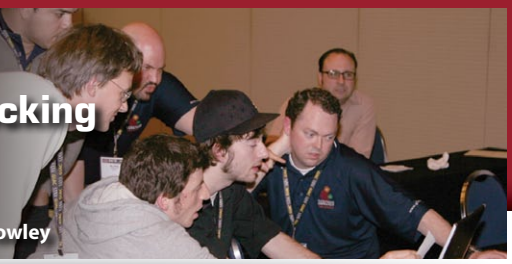
Cyber Guardian Program
www.sans.org/cyber-guardian

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS Institute's week-long Securing Windows and Resisting Malware course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. Jason blogs about Windows Security Issues on the SANS Windows Security Blog (**www.sans.org/windows-security**).

Security 560

Network Penetration Testing and Ethical Hacking



Six-Day Program • Mon, Oct 29 - Sat, Nov 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Christopher Crowley

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Who Should Attend:

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective. The final portion of the class includes a comprehensive hands-on exercise, following all of the steps to conduct a penetration test against a hypothetical target organization.

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

What Students Are Saying

"The exercises got more exciting and complicated as the week progressed, we were truly improving our skills."

-Hunter Hutcheson, USMA

Christopher Crowley *SANS Instructor*

Mr. Crowley has 10 years industry experience managing and securing networks. He has GSEC, GCIA, GCIH (gold), GCFA, and CISSP certification. His teaching experience includes GSEC, GCIA, and GCIH Mentor; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, "The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities."

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Security 579 *NEW COURSE!*

Virtualization and Private Cloud Security

Six-Day Program • Mon, Oct 29 - Sat, Nov 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Provided During Class • Instructor: Paul A. Henry

For SEC579 Virtualization and Private Cloud Security courses conducted in the United States, a Laptop will be provided for class use. However, for International events and Onsite Classes, a Hard Drive will be provided for class use.

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

Who Should Attend:

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

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

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

The class starts out with two days of architecture and security design for both virtualization and private cloud infrastructure. The next two days will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. The final two days go into detail on offense and defense - how can we virtualize environments using scanning and pen testing tools and techniques, and how do things change when we move to a cloud model?

Paul A. Henry *SANS Certified 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 principle 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 642 *NEW COURSE!*

Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Oct 29 - Sat, Nov 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Kevin Johnson

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate the you in the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag (CtF) event, which tests the knowledge you will have acquired the previous five days.

We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real world applications.

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

Who Should Attend:

- Web penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information packed advanced pen testing course will wrap up with a full day Capture the Flag (CtF) event. This CtF will target an imaginary organization's web applications and will include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.

The SANS promise is that you will be able to use these ideas immediately upon returning to the office in order to better perform penetration tests of your web applications and related infrastructure. This course will enhance your exploitation and defense skill sets as well as fulfill a need to teach more advanced techniques than can be covered in the foundational course, Security 542: Web Application Penetration Testing and Ethical Hacking.

Kevin Johnson *SANS Senior Instructor*

Kevin Johnson is a security consultant and founder of Secure Ideas. Kevin came to security from a development and system administration background. He has many years of experience performing security services for Fortune 100 companies, and in his spare time he contributes to a large number of open source security projects. Kevin's involvement in open-source projects is spread across a number of projects and efforts. He is the founder of many different projects and has worked on others. He founded BASE, which is a web front-end for Snort analysis. He also founded and continues to lead the SamuraiWTF live DVD. This is a live environment focused on web penetration testing. He also founded Yokoso! and Laudanum, which are focused on exploit delivery. Kevin is a certified instructor for SANS and the author of Security 542: Web Application Penetration Testing and Ethical Hacking. He also presents at industry events, including DEFCON and ShmooCon, and for various organizations, like Infragard, ISACA, ISSA, and the University of Florida.

Forensics 508 **BRAND NEW!**

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Mon, Oct 29 - Sat, Nov 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Alissa Torres

Over the past two years, we have seen a dramatic increase in sophisticated attacks against nearly every type of organization. Economic espionage in the form of cyber-attacks, also known as the Advanced Persistent Threat (APT), has proven difficult to suppress. Attackers from Eastern Europe and Russia continue to steal credit card and financial data resulting in millions of dollars of losses. Hackivist groups attacking government and Fortune 500 companies are becoming bolder and more frequent.

FOR508: ADVANCED COMPUTER FORENSIC ANALYSIS AND INCIDENT RESPONSE will give you help you start to become a master of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, the advanced persistent threat, and complex digital forensic cases.

This course utilizes as uses the popular SIFT Workstation to teach investigators how to investigate sophisticated crimes. The free SIFT Workstation can match any modern forensic tool suite. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

FIGHT CRIME. UNRAVEL INCIDENTS... ONE BYTE AT A TIME.

You will receive with this course: Free SANS Investigative Forensic Toolkit (SIFT) Advanced

The SIFT Advanced Toolkit consists of:

- **SIFT Workstation Virtual Machine used with many of the class hands-on exercises**
- **F-Response TACTICAL**
  - **TACTICAL enables investigators to access physical drives and physical memory of a remote computer via the network**
  - **Gives any forensic tool the capability to be used across the enterprise**
  - **The SIFT Workstation is pre-configured to leverage F-Response enterprise capabilities**
  - **Perfect for intrusion investigations and data breach incident response situations**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **Course DVD loaded with case examples, tools, and documentation**

Alissa Torres *SANS Instructor*

Alissa Torres currently works as a security researcher for KEYW Corporation in Maryland and has 10 years technical expertise in the information technology field. Previously, she was a digital forensic investigator on a government contractor security team. She has extensive experience in information security, spanning government, academic and corporate environments and holds a Bachelor's degree from University of Virginia and a Master's from University of Maryland in Information Technology. Alissa taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), teaching incident response and network basics to security professionals entering the forensics community. In addition, she has presented at various industry conferences and currently holds the following industry certifications: GCFA, CISSP, EnCE.

Who Should Attend:

- **Incident response team members**
- **Experienced digital forensic analysts**
- **Law Enforcement Officers, Federal agents, or detectives**
- **Media exploitation analysts**
- **Red team members, penetration testers, and exploit developers**
- **Information security professionals**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Management 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Oct 29 - Fri, Nov 2
9:00am - 6:00pm (Days 1-4) • 9:00am - 5:00pm (Day 5)
33 CPE/CMU Credits • Laptop NOT Required
Instructor: Stephen Northcutt

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

Knowledge Compression™ uses specialized material, in-class reviews, examinations, and test-taking training to ensure that students have a solid understanding of the material that has been presented to them.

Who Should Attend:

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

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security + 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/chicago-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

There are three goals for this course and certification:

1) Establish a minimum standard for IT security knowledge, skills, and abilities.

2) Establish a minimum standard for IT management knowledge, skills, and abilities.

3) Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us.

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a postgraduate level IT security college (**www.sans.edu**). 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. He is the lead author for Execubytes, a monthly newsletter that covers both technical and pragmatic information for security managers. He leads the MGT512 Alumni forum, where hundreds of security managers post questions. He is the lead author/instructor for MGT512, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570, and he also is the lead author/instructor for MGT421. Stephen also blogs at the SANS Security Leadership blog. **www.sans.edu/research/leadership-laboratory**

MANAGEMENT SKILL-BASED COURSE

Management 433
Securing The Human: Building and Deploying an Effective Security Awareness Program

Two-Day Course • Sat, Oct 27 - Sun, Oct 28 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop NOT Required • Instructor: Lance Spitzner, SANS Certified Instructor

Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. From RSA and Epsilon to Oak Ridge National Labs and Google, the simplest way for cyber attackers to bypass security is to target your employees. One of the most effective ways to secure the human is an active awareness and education program that goes beyond compliance and changes to behaviors. In this challenging course you will learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes your organization both more secure and compliant. In addition, you will develop metrics to measure the impact of your program and demonstrate value. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so you can immediately implement your customized awareness program upon returning to your organization.

Who Should Attend:

- Security awareness training officers
- Chief Security Officers (CSOs) and security management
- Security auditors, governance, and compliance officers
- Training, human resources and communications staff
- Organizations regulated by HIPAA, FISMA, FERPA,PCI-DSS, ISO/IEC 27001, SOX, or any other compliance-driven standards.
- Anyone responsible for planning, deploying, or maintaining an awareness program

SECURITY SKILL-BASED COURSES

Security 524
Cloud Security Fundamentals

Two-Day Course • Sun, Nov 4 - Mon, Nov 5 • 9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Required • Instructor: Chris Brenton, SANS Faculty Fellow

Many organizations today are feeling pressure to reduce IT costs and optimize IT operations. Cloud computing is rapidly emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities, and many more IT functions. A staggering number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

The first fundamental issue is the loss of hands-on control of system, application, and data security. Many of the existing best practice security controls that infosec professionals have come to rely on are not available in cloud environments, stripped down in many ways, or not able to be controlled by security teams. Security professionals must become heavily involved in the development of contract language and Service Level Agreements (SLAs) when doing business with Cloud Service Providers (CSPs). Compliance and auditing concern s are compounded. Control verification and audit reporting within CSP environments may be less in-depth and frequent as audit and security teams require.

Who Should Attend:

- Security personnel who are currently tasked with assessing the technical risks of cloud computing
- Network and systems administrators who currently manage private clouds or need to leverage hybrid and/or public cloud services
- Technical auditors and consultants who need to gain a deeper understanding of cloud computing and security concerns
- Security and IT managers who need to understand the risks of cloud computing and advise business management of the risks and various approaches to cloud computing

Day one topics include: Cloud computing introduction; Security challenges in the cloud; Infrastructure security in the cloud; Policy, risk, and governance for cloud computing; Compliance and legal considerations

Day two topics include: Audit and assessment for the cloud; Data security in the cloud; Identity and Access Management (IAM); Disaster Recovery and Business Continuity Planning (DR/BCP) in the cloud; Intrusion detection and incident response

What's Your Next Career Move?

Prepare for the future with a Master's Degree from STI. Enroll today!

Master of Science Degree in Information Security Management (MSISM)

MSISM courses offered at SANS Chicago 2012: MGT433 and MGT512

Master of Science Degree in Information Security Engineering (MSISE)

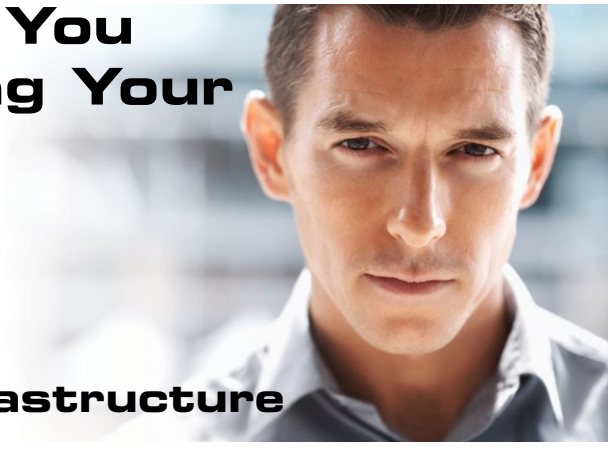
MSISE courses offered at SANS Chicago 2012: MGT433, SEC401, SEC505, SEC560, and FOR508

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu
720.941.4932

How Are You Protecting Your

- **Data**
- **Network**
- **Systems**
- **Critical Infrastructure**



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

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, audit and management.

Learn more about GIAC and how to *Get Certified* at **www.giac.org**

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

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, get the most for your training dollar, and hear from the voices that matter in computer security.

Securing The Kids *Lance Spitzner*

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century, they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even know they exist. In this one hour presentation we cover the top three risks to kids online and the top five steps you can take to protect them. This course is based on the experiences and lessons learned from a variety of SANS top instructors who not only specialize in security, but are parents just like you. This talk is sponsored and delivered by SANS Securing The Human program.

Securing The Human *Lance Spitzner*

Organizations have traditionally invested most of their security in technology, with little effort in protecting their employees. As a result, many attackers today target the weakest link, the human. Awareness, not just technology, has become key to reducing risk and remaining compliant. This high-level talk, designed for management, explains why humans are so vulnerable, how they are being actively exploited and what organizations can do about it. This presentation is not just the typical hand waving about our "State of Insecurity", it offers sound solutions that are straight forward and field proven. Many organizations are busy being busy, managing all kinds of projects and initiatives. They have all the right products. They have more logs than they know what to do with, yet the uncomfortable question persists, "is it working?" If one click by a user is all it takes, we need to re-evaluate.

GIAC Program Overview

SANS Technology Institute Open House

Vendor Events

SANS Chicago 2012

Vendor Expo

Tuesday, October 30, 2012
12:00pm - 1:30pm and 5:00pm - 7:00pm

Given that (virtually) everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS Training Event learning experience. Leading solutions providers will be on-hand for a one-day vendor expo, an added bonus to registered training event attendees.

SANS Training Options

Training Events

www.sans.org/security-training/bylocation/index_all.php

Community SANS

Live Training in Your Community

www.sans.org/community

OnSite

Live Training at Your Location

www.sans.org/onsite

Mentor

Intimate Live Instruction

www.sans.org/mentor

Summit Series

Live IT Security Summits and Training

www.sans.org/summit

OnDemand

All the Course Content at Your Own Pace

www.sans.org/ondemand

vLive

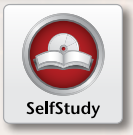
Virtual Live Training from Your Home or Office

www.sans.org/virtual-training/vlive

Simulcast

Attend Event Training From Your Location

www.sans.org/virtual-training/event-simulcast
www.sans.org/virtual-training/custom-simulcast



SelfStudy

Independent Study with Books and MP3s

www.sans.org/selfstudy

Future SANS Training Events

SANS Virginia Beach 2012

Virginia Beach, VA
August 20-31, 2012
www.sans.org/virginia-beach-2012

SANS Crystal City 2012

Arlington, VA
September 6-11, 2012
www.sans.org/crystal-city-2012

SANS Network Security 2012

Las Vegas, NV | September 16-24, 2012
www.sans.org/network-security-2012

SANS CyberCon 2012

Virtual Conference | October 8-13, 2012
www.sans.org/cybercon-2012

SANS Seattle 2012

Seattle, WA
October 14-19, 2012
www.sans.org/seattle-2012

SANS Baltimore 2012

Baltimore, MD | October 15-20, 2012
www.sans.org/baltimore-2012

SANS San Diego 2012

San Diego, CA | November 12-17, 2012
www.sans.org/san-diego-2012

SANS San Antonio 2012

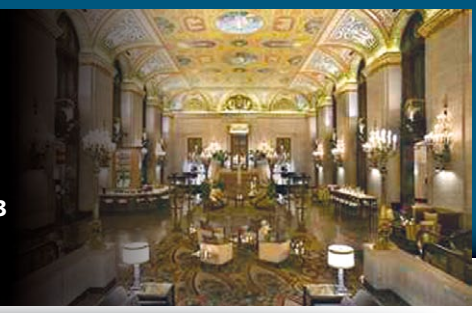
San Antonio, TX
November 27 - December 2, 2012
www.sans.org/san-antonio-2012

SANS Cyber Defense Initiative 2012

Washington, DC | December 7-16, 2012
www.sans.org/cyber-defense-initiative-2012

SANS Chicago 2012

Hotel Information



Conference Location
The Palmer House Hilton
17 East Monroe Street | Chicago, IL, 60603
Tel: 312-726-7500
www.palmerhousehiltonhotel.com

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 5, 2012. To make reservations please call 800-445-8667 and ask for the SANS group rate.

Note: You must mention that you are attending the SANS Institute training event to get the discounted rate or special amenities (such as complimentary high-speed internet) in your room. If you book outside the SANS block or stay at another hotel SANS has no influence on the terms and conditions you agreed to when making a reservation.

The hotel will require a major credit card to guarantee your reservation. To cancel your reservation, you must notify the hotel at least 72 hours before your planned arrival date.

Top 5 reasons to stay at The Palmer House Hilton

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at The Palmer House Hilton, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at The Palmer House Hilton that you won't want to miss!
5. Everything is in one convenient location!

SANS Chicago 2012

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/chicago-2012

To register, go to www.sans.org/chicago-2012

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 9:00am - 8:00pm Eastern Time.

Cancellation

You may substitute another person in your place at any time by e-mail: **registration@sans.org** or faxing to 301-951-0140. There is a $300 cancellation fee per registration. Cancellation requests must be received by Wed, October 3 by fax or mail-in order to receive a refund.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**9/12/12**	**$500.00**	**9/26/12**	**$250.00**

Discount applies to five- and six-day courses only.

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.php** prior to registering.

SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year. The SANS Discount Program that pays you credits and delivers flexibility
www.sans.org/vouchers

Scan the QR code to register by September 12th and

SAVE $500

on Chicago courses.

www.sans.org/info/109915

To download a free QR reader
www.mobile-barcodes.com/qr-code-software

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

Register using this Promo Code

Save $500 when you register by September 12th
www.sans.org/chicago-2012