SANS

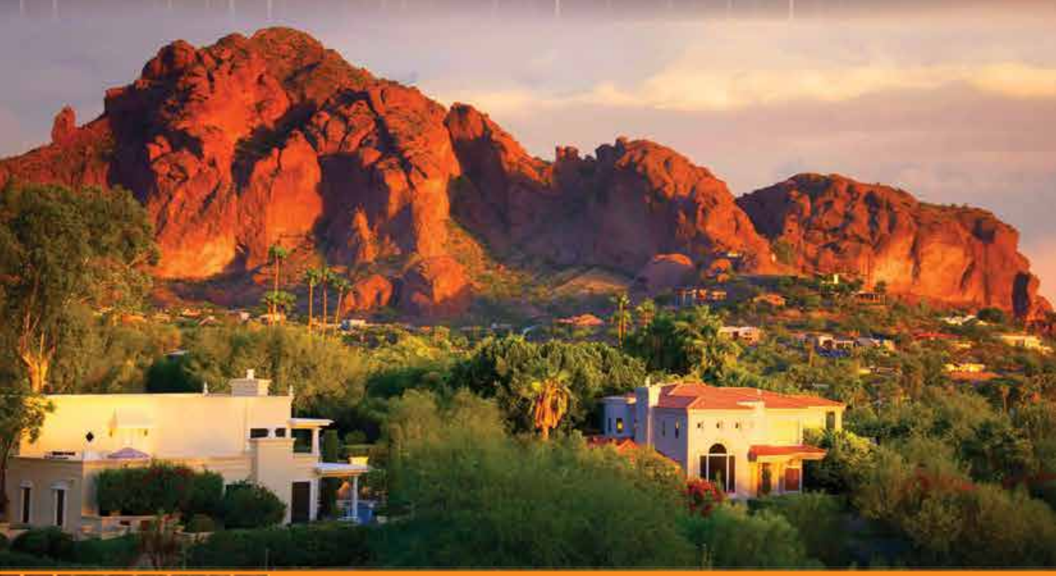
THE MOST TRUSTED SOURCE FOR INFORMATION AND SOFTWARE SECURITY TRAINING

Scottsdale 2013

February 17-23, 2013

SANS Exceptional Training comes to Scottsdale

> "Cutting edge, extremely knowledgeable and elite instructors, very comprehensive breadth."
> -CHARLES BENAGH, NORTHROP GRUMMAN



Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Security Leadership Essentials For Managers with Knowledge Compression™

Mobile Device Security and Ethical Hacking

Implementing and Auditing the Twenty Critical Security Controls – In-Depth

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

GIAC Approved Training

Dear Colleague,

I am pleased to invite you to join me at our new campus in Arizona this February. We have moved from Phoenix to the Hilton Scottsdale Resort & Villas in nearby Scottsdale. Along with me, the training team of Dr. Eric Cole, Ed Skoudis, and James Tarala will be doing their best to present the security management and IT security training you need at **SANS Scottsdale 2013 on February 17-23**. See below what we are teaching!

Stephen Northcutt

Three of our courses align with *DoD Directive 8570*, and they are associated with *GIAC Certification*. To learn more, visit the GIAC page and register for your certification attempt today. These same courses can also lead to a Master's Degree at SANS Technology Institute (STI). Take classes in Information Security Management (MSISM) or Engineering (MSISE). See our STI page for more information and apply today!

Our SANS Scottsdale 2013 campus is the **Hilton Scottsdale Resort & Villas** in the heart of the city. This hotel has views of Camelback Mountain, and it is close to shopping, dining, attractions, and world-class golf. Within 25 miles are the Arizona State Capitol, Camelback Mountain, Chase Field, Desert Botanical Gardens, Heard Museum (American Indian arts/culture), Phoenix Art Museum, Phoenix Zoo, Pueblo Grande Museum, Taliesin West, and a western town called Rawhide! Scottsdale's average high temperature in February is 73 degrees, so this might be a nice winter break.

A special discounted rate of $179.00 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 January 25, 2013. See our location page for complete information.

Register and pay by January 2 and save $500. Start making your training and travel plans now; let your colleagues and friends know about SANS Scottsdale 2013. We look forward to seeing you there.

Kind regards,

Stephen Northcutt
President
SANS Technology Institute, a postgraduate computer security college

Here is what SANS Alumni have had to say about their SANS event training experience:

"I highly advise anyone requiring this level of training to get it through SANS. The instructors share information and insight not found elsewhere."
-Clifton Dickens,
Richmond Public Schools

"Excellent course. Very thorough coverage of the advertised materials and concepts. Excellent instructor, as expected, and an excellent time. As always, SANS delivers."
-Kevin McLaughlin,
University of Cincinnati

"This (my first SANS course) is the best training course I've ever taken in 20 years of IT work. I am very impressed, and look forward to taking more courses."
-Justin Brown, OOK Consulting

Courses-at-a-Glance

		SUN 2/17	MON 2/18	TUE 2/19	WED 2/20	THU 2/21	FRI 2/22	SAT 2/23
SEC401	SANS Security Essentials Bootcamp Style	PAGE 1						
SEC504	Hacker Techniques, Exploits & Incident Handling		PAGE 2					
SEC566	Implementing and Auditing the Twenty Critical Security Controls – In-Depth		PAGE 3					
SEC575	Mobile Device Security and Ethical Hacking		PAGE 4					
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™		PAGE 5					

Security 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Sun, Feb 17 - Fri, Feb 22
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

It seems wherever you turn organizations are being broken into and the fundamental question that everyone wants to know is Why? Why do some organizations get broken into and others do 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 be given 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**
- **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 how well they are at the 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 spend a dollar of its IT budget or allocates any resources or time on 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

BOOTCAMP

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

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

Security is all about making sure you are focusing in 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 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.

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus in on the right areas of security by building out a dynamic defense. 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 the 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. Dr. Cole is an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services and leads research and development initiatives to advance the state-of-the-art in information systems security.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Security 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Feb 18 - Sat, Feb 23
9:00am - 5:00pm • 37 CPE/CMU Credits
Laptop Required • Instructor: Ed Skoudis

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors and the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

Who Should Attend:

- **Incident handlers**
- **Penetration testers**
- **Ethical hackers**
- **Leaders of incident handling teams**
- **System administrators who are on the front lines defending their systems and responding to attacks**
- **Other security personnel who are first responders when systems come under attack**

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is the founder of Counter Hack Challenges, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including NetWars, Cyber Quests, and Cyber Foundations. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in financial, high technology, healthcare, and other industries.

Ed conducted a demonstration of hacker techniques against financial institutions for the United States Senate and is a frequent speaker on issues associated with hacker tools and defenses. He has published numerous articles on these topics as well as the Prentice Hall best sellers ***Counter Hack Reloaded*** and ***Malware: Fighting Malicious Code***. Ed was also awarded 2004-2009 Microsoft MVP awards for Windows Server Security and is an alumnus of the Honeynet Project. Previously, Ed served as a security consultant with International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips.
http://blog.commandlinekungfu.com

> ***"In-depth, complete course that teaches all you need to know about exploits."***
> -Stephan Harrison,
> Naval Air Warfare Center

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Security 566

Implementing and Auditing the Twenty Critical Security Controls - In-Depth

Five-Day Program • Mon, Feb 18 - Fri, Feb 22
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

In the last couple of years it has become obvious that in the world of information security, the offense is outperforming the defense. Even though budgets increase and management pays more attention to the risks of data loss and system penetration, data is still being lost and systems are still being penetrated. Over and over people are asking, "What can we practically do to protect our information?" The answer has come in the form of 20 information assurance controls. **www.sans.org/critical-security-controls/guidelines.php**

This course has been written to help those implementing or deploying a strategy for information assurance in their agency or organization by enabling them to better understand these guidelines. Specifically the course has been designed in the spirit of the offense teaching the defense to help security practitioners understand not only what to do to stop a threat, but why the threat exists and how later to audit to ensure that the organization is indeed in compliance with their standards.

And in SANS style, this course will not only provide a framework for better understanding, but will give you a hands-on approach to learning these objectives to ensure that what you learn today, you'll be able to put into practice in your organization tomorrow.

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. These Top 20 Security Controls, listed below, are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all security-conscious organizations.

The US military and other government and private organizations, including the National Security Agency (NSA), Department of Homeland Security (DHS), and the U.S. Government Accountability Office (GAO) defined these top 20 controls as their consensus for the best way to block the known attacks and help find and mitigate damage from the attacks that get through.

For security professionals, the course enables you to see how to put the controls in place in your existing network though the effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers the course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. It closely reflects the Top 20 Critical Security Controls.

Who Should Attend:

- **Information assurance auditors**
- **System implementers or administrators**
- **Network security engineers**
- **IT administrators**
- **Department of Defense (DoD) personnel or contractors**
- **Federal agencies or clients**
- **Private sector organizations looking to improve information assurance processes and secure their systems**
- **Security vendors and consulting groups looking to stay current with frameworks for information assurance**

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

> ***"The course provides a good framework for how to implement the Top 20 controls in a systematic way."***
> -Mike Schaub, Constellation Energy Nuclear Group

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 times performs independent security audits and assists internal audit groups to develop 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.

Security 575

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, Feb 18 - Sat, Feb 23
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Peter Szczepankiewicz

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

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.

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**

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

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 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.

Peter Szczepankiewicz *SANS Certified Instructor*

Formerly working with the military, Peter responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a Senior Security Engineer with IBM. People lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. Peter expounds, "Putting together networks only to tear them apart, is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place."

> *"Wow. This course is everything you need to know about mobile device deployment, risks and more. Don't deploy your mobile devices without taking this course first!"*
> -Bryan Simon, INTEGRIS Credit Union

Management 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Feb 18 - Fri, Feb 22
9:00am - 6:00pm (Days 1-4) • 9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits • Laptop Not Needed • 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 gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

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.

Who Should Attend:

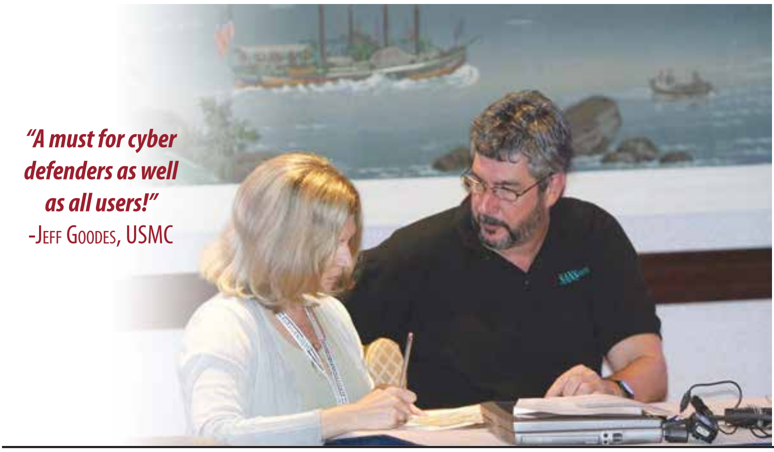
- **All newly-appointed information security officers**
- **Technically-skilled administrators that have recently been given leadership responsibilities**
- **Seasoned managers that want to understand what your technical people are telling you**

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute. Stephen is author/coauthor of ***Incident Handling Step-by-Step***, ***Intrusion Signatures and Analysis***, ***Inside Network Perimeter Security*** 2nd Edition, ***IT Ethics Handbook***, ***SANS Security Essentials***, ***SANS Security Leadership Essentials***, and ***Network Intrusion Detection*** 3rd edition. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer.

Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings. He leads the Management 512 Alumni Forum, where hundreds of security managers post questions. He is the lead author/instructor for Management 512: SANS Security Leadership Essentials for Managers, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570. He also is the lead author/instructor for Management 514: IT Security Strategic Planning, Policy, and Leadership. Stephen blogs at the SANS Security Laboratory.
www.sans.edu/research/security-laboratory

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



"A must for cyber defenders as well as all users!"
-Jeff Goodes, USMC

www.giac.org

www.sans.edu

Special Events

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.

Keynote: Unleashing the Dogs of (cyber) War *Ed Skoudis*

With the onslaught of recent headlines containing revelations of nation-state activity in computer attacks, a lot of people are wondering: What the heck is going on? Although controversial in some quarters, the militarization of cyber space proceeds apace. Some think that military operations in cyber space are impossible, impractical, or just plain evil. In this lively and hard-hitting presentation, Ed Skoudis will analyze the trends and look at where such activities may be heading. We'll then focus on some of the ramifications for the hacker community. How could cyber military action impact you and your hacking research? What steps should hackers take to prepare for a significantly more militarized cyber space? We'll discuss those issues, and many more.

Information Security Metrics: Practical Steps to Measurement

James Tarala

Show up to a security presentation, walk away with a specific action plan. In this presentation, James Tarala, a senior instructor with the SANS Institute, will be presenting on making specific plans for information assurance metrics in an organization. Clearly this is an industry buzzword at the moment when you listen to presentations on the 20 Critical Controls, NIST guidance, or industry banter). Security professionals have to know that their executives are discussing the idea. So exactly how do you integrate information assurance metrics into action in an organization and actually achieve value from the effort. Learn what efforts are currently underway in the industry to create consensus metrics guides and what initial steps an organization can take to start measuring the effectiveness of their security program. Small steps are better than no steps, and by the end of this presentation, students will have a start integrating metrics into their information assurance program.

APT: It is Not Time to Pray, It is Time to Act *Dr. Eric Cole*

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

GIAC Program Overview *Stephen Northcutt*

SANS Technology Institute Brief *President Stephen Northcutt*

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.

GIAC Certification opportunities being offered at this event:

CERT	CERT DESCRIPTION	SANS COURSE
GSEC	GIAC Security Essentials	SEC401
GCIH	GIAC Certified Incident Handler	SEC504
GSLC	GIAC Security Leadership	MGT512

> *"GIAC is the only certification that proves you have hands-on technical skills."*
>
> -Christina Ford, Department of Commerce

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

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.

STI offers two master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

New cohorts begin in January at
SANS Security East 2013 (New Orleans)
and in September at
SANS Network Security 2013 (Las Vegas).
Learn more about STI Cohorts at
www.sans.edu/interest/cohort

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu
720.941.4932

3 of the courses being offered at SANS Scottsdale 2013 may be applied towards an STI Master's Degree.

SANS CYBER GUARDIAN PROGRAM

www.sans.org/cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

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.

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

Program Prerequisites

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

Core Courses

SEC503	Intrusion Detection In-Depth (GCIA)
SEC504	Hacker Techniques, Exploits, and Incident Handling (GCIH)
SEC560	Network Penetration Testing and Ethical Hacking (GPEN)
FOR508	Advanced Computer Forensic Analysis & Incident Response (GCFA)

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

Blue Team Courses

SEC502	Perimeter Protection In-Depth (GCFW)
SEC505	Securing Windows and Resisting Malware (GCWN)
SEC506	Securing Linux/Unix (GCUX)

Red Team Courses

SEC542	Web App Penetration Testing and Ethical Hacking (GWAPT)
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
SEC660	Advanced Penetration Testing, Exploits, and Ethical Hacking (GXPN)

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

Future SANS T

SANS Cyber Defense Initiative 2012

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

SANS Mobile Device Security Summit 2013

Anaheim, CA | January 7-14, 2013
www.sans.org/event/mobile-device-security-summit-2013

SANS Virtualization and Cloud Computing Summit 2013

Anaheim, CA | January 7-14, 2013
www.sans.org/event/virtualization-cloud-summit-2013

SANS Security East 2013

New Orleans, LA
January 16-23, 2013
www.sans.org/event/security-east-2013

SANS North American SCADA and Process Control Summit 2013

Lake Buena Vista, FL | February 6-15, 2013
www.sans.org/event/north-american-scada-2013

SANS 2013

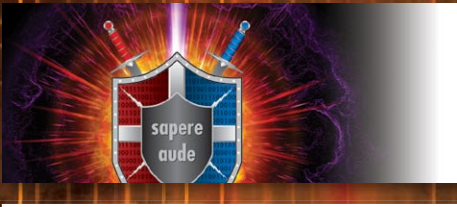
Orlando, FL
March 8-15, 2013
www.sans.org/event/sans-2013

SANS Monterey 2013

Monterey, CA
March 22-27, 2013
www.sans.org/event/monterey-2013

SANS Northern Virginia 2013

Reston, VA
April 8-13, 2013
www.sans.org/event/northern-virginia-2013



SANS Cyber Guardian 2013

Baltimore, MD
April 15-20, 2013
www.sans.org/event/cyber-guardian-2013

raining Events

SANS **AppSec** Summit 2013

Austin, TX
April 22-27, 2013

www.sans.org/event/appsec-2013

SANS **Security West** 2013

San Diego, CA
May 9-14 2013

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

SANS **Austin** 2013

Austin, TX
May 19-24 , 2013

www.sans.org/event/austin-2013

SANSFIRE 2013

Washington, DC
June 13-23, 2013

www.sans.org/event/sansfire-2013

SANS **Digital Forensics & Incident Response** Summit 2013

Austin, TX | July 9-16, 2013

www.sans.org/event/dfir-summit-2013

SANS **Rocky Mountain** 2013

Denver, CO
July 15-22, 2013

www.sans.org/event/rocky-mountain-2013

SANS **San Francisco** 2013

San Francisco, CA
July 29 - August 4, 2013

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

SANS **Boston** 2013

Boston, MA
August 12-17, 2013

www.sans.org/event/boston-2013

SANS **Network Security** 2013

Las Vegas, NV
September 18-25, 2013

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

SECURITY AWARENESS

FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Includes videos, newsletters, posters and screen savers .
- Create your own program by choosing from 30 different training modules.
- Training meets mandated compliance requirements including PCI DSS, HIPAA, FERPA, FISMA, SOX and ISO 27001.
- Offered in over 20 languages.
- Host on SANS VLE or on your own LMS.
- For a free trial, visit us at www.securingthehuman.org or contact info@securingthehuman.org for more information.

SANS SECURING THE HUMAN

www.securingthehuman.org

SANS Scottsdale 2013

Hotel Information

Conference Location
Hilton Scottsdale Resort and Villa

6333 North Scottsdale Road | Scottsdale , AZ
Tel: 480-948-7750
www3.hilton.com/en/hotels/arizona/hilton-scottsdale-resort-and-villas-SCTSHHF/index.html

Special Hotel Rates Available

A special discounted rate of $179.00 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 January 25, 2013. To make reservations please call (800) HILTONS (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 Hilton Scottsdale Resort & Villas

1 All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.

2 No need to factor in daily cab fees and the time associated with travel to alternate hotels.

3 By staying at the Hilton Scottsdale Resort & Villas, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.

4 SANS schedules morning and evening events at the Hilton Scottsdale Resort & Villas that you won't want to miss!

5 Everything is in one convenient location!

SANS Scottsdale 2013

Registration Information

SANS
The Most Trusted Source for Information and Software Security Training

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

Register online at www.sans.org/event/scottsdale-2013

To register, go to www.sans.org/event/scottsdale-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 January 30, 2013. There is a $300 cancellation fee per registration.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**1/2/13**	**$500.00**	**1/16/13**	**$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.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