SANS San Diego 2012

November 12-17, 2012

The Most Trusted Source for Information and Software Security Training

Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits & Incident Handling

SANS Security Leadership Essentials for Managers with Knowledge Compression™

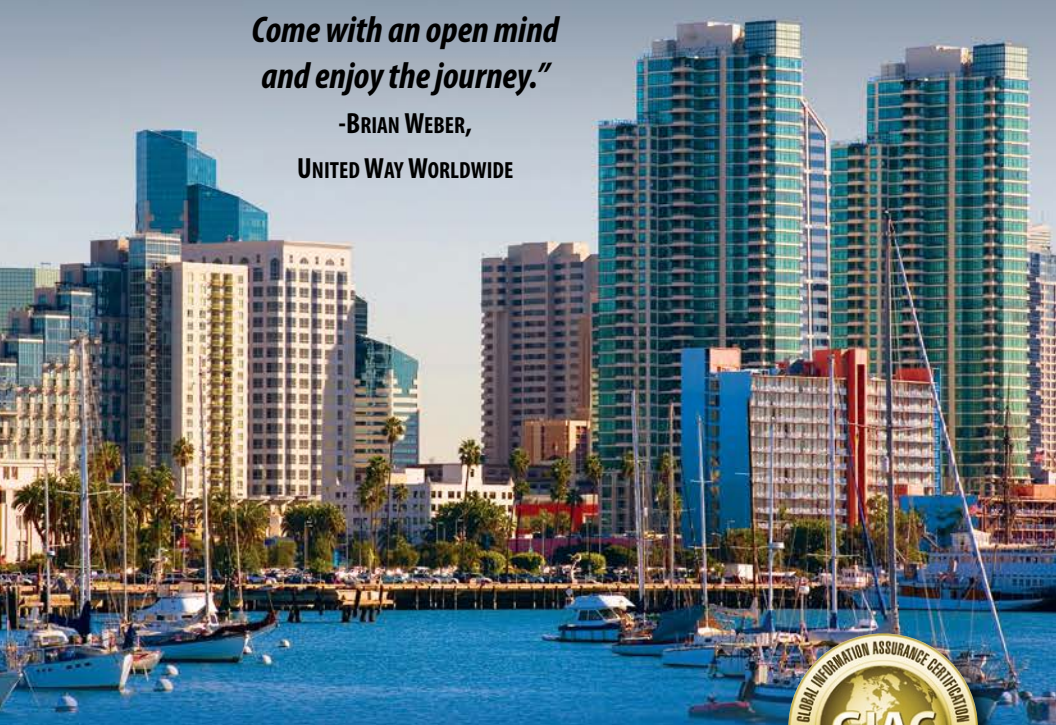
Computer Forensic Investigations – Windows In-Depth

Defending Web Applications Security Essentials

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

"The real deal. Come with an open mind and enjoy the journey."

-Brian Weber, United Way Worldwide



Register at www.sans.org/san-diego-2012

GIAC Approved Training

Dear Colleague,

I am pleased to invite you to **SANS San Diego 2012 on November 12-17 located at the Hard Rock Hotel!** Don't miss the chance for a late fall trip to Southern California and get the best of SANS training in security management, IT security or computer forensics. You will return home with valuable, hands-on, security skills!

Our hand-picked instructor lineup includes Dr. Eric Cole, James Tarala, Mike Poor, Michael Murr, and me! See this brochure for a complete schedule, course descriptions, instructor bios, GIAC cert availability for four of our courses, and information about earning your Master's Degree in Information Security through the SANS Technology Institute (STI). Don't miss our bonus evening talks – these hot, late-breaking sessions are presented by our instructors and will add to your experience at no additional cost.

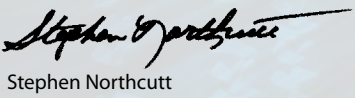
Hard Rock Hotel San Diego is located at the entrance to the Gaslamp Quarter. From the website for the hotel: "Whether you're coming for business or pleasure, the Hard Rock Hotel San Diego looks forward to providing their guests with an authentic experience that rocks!" See our *Hotel and Travel Information* page for more details.

San Diego is an awesome destination with November average temps reaching 70 degrees. There are so many things to do, and here are a few things that are happening during the week of SANS San Diego 2012:

- **Hotel del Coronado Historic Walking Tour, Coronado Visitor Center and Historical Association & Museum – Location: Coronado**
- **"GROSSOLOGY: The (Impolite) Science of the Human Body" returns to the Fleet! - Reuben H. Fleet Science Center – Location: Balboa Park**
- **"How Things Fly", San Diego Air & Space Museum – Location: Balboa Park**
- **1/2 Day Fishing Trips from Fisherman's Landing – Location: Harbor Island**
- **November 2–12: San Diego Beer Week (come early!)**
- **November 14-18: 9th Annual San Diego Bay Wine & Food Festival**
- **Starting November 17: SeaWorld's Christmas Celebration 2012, SeaWorld San Diego – Location: Mission Bay**
- **November - December: Dr. Seuss' "How the Grinch Stole Christmas!" This annual holiday musical jumps right off the pages of the classic Dr. Seuss book and onto the stage of The Old Globe theatre in Balboa Park.**

Register and pay by Wednesday, October 3, to receive a $500 discount. Start making your training and travel plans now and let your colleagues and friends know about SANS San Diego 2012. We look forward to seeing you there.

Best regards,



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

Stephen Northcutt

Here is what past attendees had to say about their SANS 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

"Good coverage, relevant content, great instructor. A lot of material covered but Mike Poor made it manageable. Facilitators, instructors, and SANS personnel were very helpful all around. Thank you!"
-Carmencita Muramoto, Raytheon Company

"If you want to pass a test, take a bootcamp. If you want to understand the technology and work with experts on the subject, take a SANS course."
-Justin Grace, Texas Air National Guard

Courses-at-a-Glance

		MON 11/12	TUE 11/13	WED 11/14	THU 11/15	FRI 11/16	SAT 11/17
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					
SEC579	Virtualization and Private Cloud Security	PAGE 4					
DEV522	Defending Web Applications Security Essentials	PAGE 5					
FOR408	Computer Forensic Investigations - Windows In-Depth	PAGE 6					
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	PAGE 7					

Security 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, Nov 12 - Sat, Nov 17
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.

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

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).

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 for 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 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.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Security 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Nov 12 - Sat, Nov 17
9:00am - 5:00pm • 37.5 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

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.

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

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.

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your company's system and also that you advise your network and computer operations teams of your testing.

What Students Are Saying

"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

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling ***Snort*** series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Security 566

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

Five-Day Program • Mon, Nov 12 - Fri, Nov 16
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 known as the Consensus Audit Guidelines (CAG), located at **www.sans.org/critical-security-controls/guidelines.php**.

Who Should Attend:

- Information assurance auditors
- System implementers/administrators
- Network security engineers
- IT administrators
- DoD personnel/contractors
- Federal agencies/clients
- Private sector organizations looking for information assurance priorities for securing their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD 440, SEC401, SEC501, SANS Audit classes, and MGT512

This course has been written to help those setting/implementing/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 how 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. Walking away from this course, students should better understand how to create a strategy for successfully defending their data, implement controls to prevent their data from being compromised, and audit their systems to ensure compliance with the standard. And in SANS style, this course will not only provide a framework for better understanding, but also 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.

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

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 are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block the known attacks and the best way to 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 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 found at **www.sans.org/critical-security-controls/guidelines.php**.

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 579

Virtualization and Private Cloud Security

Six-Day Program • Mon, Nov 12 - Sat, Nov 17
9:00am - 5:00pm • 36 CPE/CMU Credits
***Laptop Provided For Class Use* • Instructor: Dave Shackleford**

For the SEC579: Virtualization and Private Cloud Security course, a laptop 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.

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.

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

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.

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

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 assess virtualized environment using scanning and pen testing tools and techniques, and how do things change when we move to a cloud model?

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant at Voodoo Security; senior vice president of research and CTO at IANS; and a SANS analyst, instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft; CTO for the Center for Internet Security; and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the coauthor of Hands-On Information Security from Course Technology as well as the Managing Incident Response chapter in the Course Technology book Readings and Cases in the Management of Information Security. Recently, Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

Developer 522

Defending Web Applications Security Essentials

Six-Day Program • Mon, Nov 12 - Sat, Nov 17
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dr. Johannes Ullrich

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

This class goes beyond classic web applications and includes coverage of Web 2.0 technologies, like AJAX and web services. We also arm you with knowledge to defend yourself against cutting-edge attackers, such as various protective HTTP headers and new generation of browser-based web application protections.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. The topics that will be covered include:

- **Infrastructure security**
- **Server configuration**
- **Authentication mechanisms**
- **Application language configuration**
- **Application coding errors like SQL injection and cross-site scripting**
- **Cross-site request forging**
- **Authentication bypass**
- **Web services and related flaws**
- **Web 2.0 and its use of web services**
- **XPATH and XQUERY languages and injection**
- **Business logic flaws**
- **Protective HTTP headers**

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

Who Should Attend:

- **Application developers**
- **Application security analysts or managers**
- **Application architects**
- **Penetration testers who are interested in learning about defensive strategies**
- **Security professionals who are interested in learning about web application security**
- **Auditors who need to understand defensive mechanisms in web applications**
- **Employees of PCI compliant organizations who need to be trained to comply with PCI requirements**

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Dr. Johannes Ullrich *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. Prior to working for SANS, Johannes worked as a lead support engineer for a Web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also maintains a daily security news summary podcast and enjoys blogging about application security.
http://software-security.sans.org/blog

Forensics 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Nov 12 - Sat, Nov 17
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Michael Murr

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 threat, 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 cybercrime law enforcement agents to piece together what happened in these cases.

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.

Who Should Attend:

- Information technology professionals
- Incident Response Team Members
- Law enforcement officers, federal agents, or detectives
- Media Exploitation Analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

FOR408: COMPUTER FORENSIC INVESTIGATIONS - WINDOWS IN-DEPTH is the first course in the SANS Computer Forensic Curriculum. If this is your first computer forensics course with SANS we recommend that you start here.

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

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

As a part of this course you will receive a SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit.

- **One Tableau T35es Write Blocker (Read-Only)**
- **IDE Cable/Adapters**
- **SATA Cable/Adapters**
- **FireWire and USB Cable Adapters**
- **Forensic Notebook Adapters (IDE/SATA)**

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS Security 504 (Hacker Techniques, Exploits, and Incident Handling), SANS Security 508 (Computer Forensics, Investigation, and Response), and SANS Forensics 610 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about Digital forensics on his Forensic Computing blog. **www.forensicblog.org**

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

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Management 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Nov 12 - Fri, Nov 16
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.

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.

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**

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.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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**

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: Future Trends in Network Security *Dr. Eric Cole*

Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance. Reactive security will no longer work. Therefore, organizations need to better understand what the future trends, risks, and threats are so that they can be better prepared to make their organizations as secure as possible. Dr. Cole's in-depth, cross-industry experience allows him to give relevant examples in every instance. This presentation covers security issues that are relevant to IT managers and administrators alike.

Practical, Efficient Unix Auditing (with Scripts) *James Tarala*

Technical audits of Unix operating system controls can scare auditors - especially if the scope is a flavor of Unix that the auditor is not 100% comfortable with the operating system. But operating system audits are the bread and butter of most IS auditors. In most every technical audit that an IS auditor will perform there will be some level of inspection that's performed at the operating system level. Auditors therefore need the skills be able to audit the technical components of an operating system, whether they have a strong background in that operating environment or not. In this presentation James Tarala, a senior instructor with the SANS Institute, will provide a practical, step by step approach to auditing Unix operating systems. Not only will students receive a better understanding of the audit process for these technical controls, but they will walk out of the presentation with access to an audit script to assist them in their efforts!

Cloud Computing and the 20 Critical Security Controls

Dave Shackleford

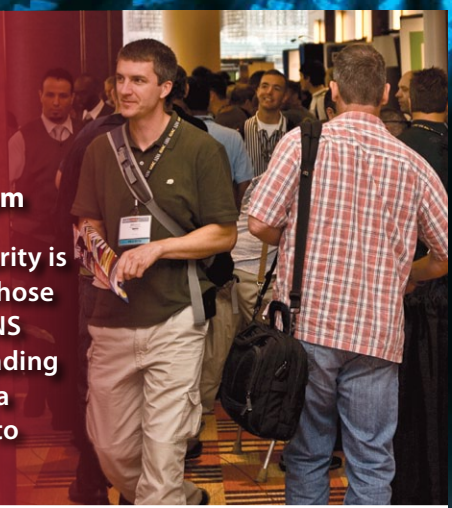
As more organizations look to leverage cloud computing providers, security is a major consideration. Today, the SANS Top 20 Critical Security Controls is considered a reasonable benchmark for security controls in most organizations. In this talk, Dave will delve into the ways cloud computing affects our security posture overall, and tie this into the latest version of SANS' Top 20 Critical Security Controls. You'll walk away with a solid understanding of how these controls can be met in relation to cloud computing, and some of the challenges for each one.

SANS San Diego 2012

Vendor Expo

Tuesday, November 13, 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.



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, audit, and management.

"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**

What's Your Next Career Move?

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

Master of Science Degree in Information Security Management (MSISM)

MSISM courses offered at SANS San Diego 2012:
DEV522 and MGT512

Master of Science Degree in Information Security Engineering (MSISE)

MSISE courses offered at SANS San Diego 2012:
SEC401, SEC504, DEV522,and FOR408

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu
720.941.4932

SANS
CYBER GUARDIAN PROGRAM
www.sans.org/cyber-guardian

Become a SANS Cyber Guardian and stay one step ahead of the threats as well as know what to do when a breach occurs.

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.

How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills with each course. 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!

Core Courses	Blue Team Courses	Red Team Courses
SEC503 • SEC504 SEC560 • FOR508	SEC502 • SEC505 SEC506	SEC542 • SEC617 SEC660

Future SANS Training Events

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

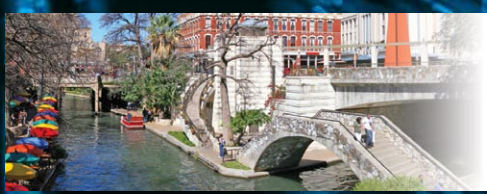
SANS CyberCon 2012
Virtual Conference

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 **Chicago** 2012
Chicago, IL
October 27 - November 5, 2012
www.sans.org/chicago-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 **Security East** 2013
New Orleans, LA
January 16-21, 2013
www.sans.org/security-east-2013

SANS Training Options

Multi-Course Training Events

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

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 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

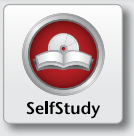
Virtual Live Training from Your Home or Office

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

SANS San Diego 2012

Hotel Information

Conference Location

Hard Rock Hotel San Diego

207 Fifth Avenue | San Diego, CA 92101
Phone: (619) 702-3000
www.hardrockhotelsd.com

Special Hotel Rates Available

A special discounted rate of $210.00 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 19, 2012. To make reservations please call (866) 751-ROCK (866-751-7625) and ask for the SANS November 12 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 Hard Rock Hotel San Diego

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 Hard Rock Hotel San Diego, 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 Hard Rock Hotel San Diego that you won't want to miss!
5. Everything is in one convenient location!

SANS San Diego 2012

Registration Information

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

Register online at www.sans.org/san-diego-2012

To register, go to www.sans.org/san-diego-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 24** by fax or mail-in order to receive a refund.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**10/3/12**	**$500.00**	**10/17/12**	**$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 October 3rd and

SAVE $500

on San Diego courses.

www.sans.org/info/110500

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 October 3rd
www.sans.org/san-diego-2012