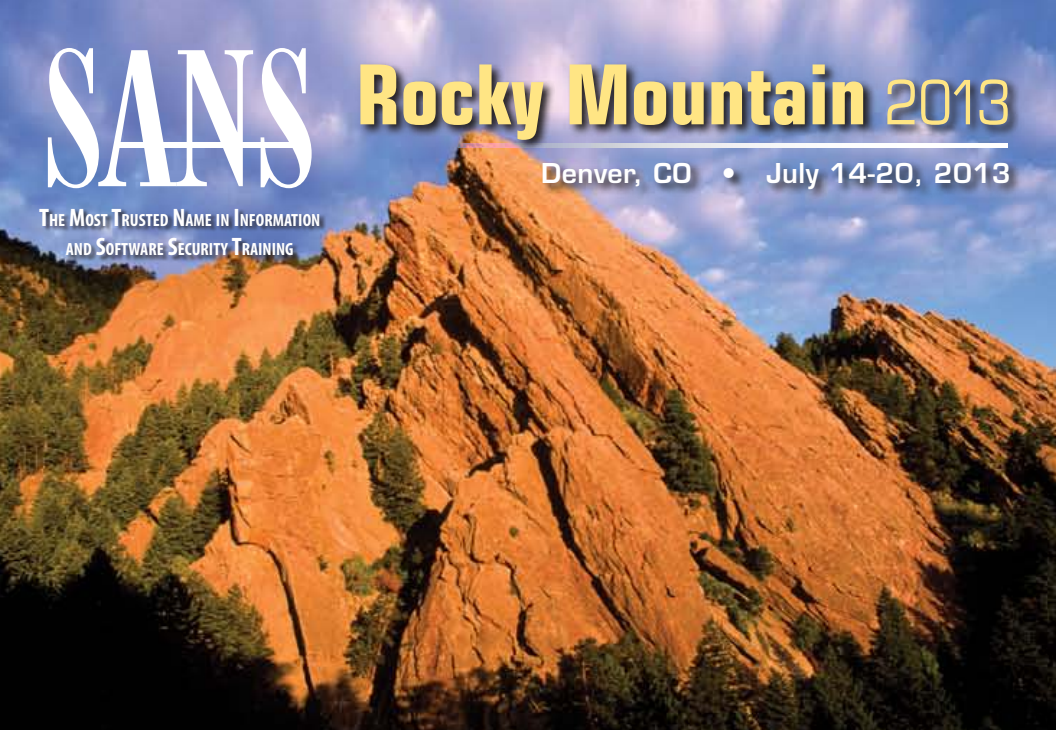
SANS Rocky Mountain 2013

Denver, CO • July 14-20, 2013

The Most Trusted Name in Information and Software Security Training



Hands-on immersion training programs, including:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Security Leadership Essentials For Managers with Knowledge Compression

Web App Penetration Testing and Ethical Hacking

Securing Windows and Resisting Malware

SANS +S Training Program for the CISSP® Certification Exam

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

"Learning from the best, comprehensive and detailed, 5 times the exercises of other classes. Intense."

-Razi Asaduddin, ExxonMobil

GIAC Approved Training

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

Dear Colleague,

Mile high...mile deep, IT security training! Why not try **SANS Rocky Mountain 2013**?

I'd like to encourage you to find out about our training event in Denver at SANS Rocky Mountain 2013 on July 14-20. We have eight five- and six-day cybersecurity courses in the security, pen testing, IT audit, and security management disciplines along with our new Securing Windows and Resisting Malware course – all in this spectacular western city. This annual event is taking place at Hyatt Regency Denver Convention Center located in the heart of downtown Denver.

Now more than ever, hands-on experience will set you apart from others in the field, so don't miss this opportunity. Our event brochure will provide all the information you need! Learn about our award-winning faculty scheduled for Rocky Mountain: Dr. Eric Cole, Stephen Northcutt, Jason Fossen, James Tarala, Dave Shackleford, Kevin Johnson, David R. Miller, and Kevin Fiscus who will team together to ensure that you not only learn the material, but that you can also use it the day you return to the office.

Also look for detailed information about our courses, faculty bios, and bonus evening events. Don't miss this chance to take one of three courses that are in alignment with the *DoD Directive 8570* (SEC401, SEC504, and MGT512). More and more students are telling us that the certifications we offer are vital to their jobs, and we'll tell you why on our *GIAC* page – seven of our courses offer GIAC Certification. Look for details about our *Vendor Showcase* (July 16) along with a great lineup of *SANS @Night* evening events. These extra sessions are free with your paid tuition and are a great enhancement to your classroom training.

In conjunction with SANS Rocky Mountain 2013, SANS will host **NetWars Tournament** competition – an intense interactive, Internet-based environment for computer attacks and defenses. NetWars will be held in the evening on July 18 and 19.

Receive a discount of up to $500 for any course paid for by Wednesday, May 29! Register today for SANS Rocky Mountain 2013! We look forward to seeing you in Denver!

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

Stephen Northcutt

Here's what past Rocky Mountain attendees had to say:

"I said it back in 2004 and it still holds true today; SANS offers the best training in the industry."
-Brian Hughes, USDA

"SEC401 is the most wide-range, comprehensive security training available! Dr. Cole's engaging, energetic teaching style draws you in, his passion for security is infectious!"
-Michael Leach, Nationwide

"If interested in security engineering or security architecture, SEC505 gives insight to necessary contacts."
-Robert Pacheco, Citizens Property Insurance Corp.

"AUD507 is very valuable for security personnel to understand the intricacies of auditing."
-Margie Marquez, B&W Technical Services

Courses-at-a-Glance

		SUN 7/14	MON 7/15	TUE 7/16	WED 7/17	THU 7/18	FRI 7/19	SAT 7/20
SEC401	Security Essentials Bootcamp Style		PAGE 1					
SEC504	Hacker Techniques, Exploits, and Incident Handling		PAGE 2					
SEC505	Securing Windows and Resisting Malware *NEW!*		PAGE 3					
SEC542	Web App Penetration Testing and Ethical Hacking		PAGE 4					
SEC566	Implementing and Auditing the Twenty Critical Security Controls – In-Depth		PAGE 5					
MGT414	SANS +S Training Program for the CISSP® Cert Exam		PAGE 6					
MGT512	Security Leadership Essentials For Managers		PAGE 7					
AUD507	Auditing Networks, Perimeters, and Systems		PAGE 8					
HOSTED	Securing Information Systems Before and After an Incident		PAGE 9					

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, July 15 - Sat, July 20
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 answered is: Why? Why do some organizations get broken into and others not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore we will teach you how to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will 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.

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in cyber security. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time 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?**

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

Who Should Attend:

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

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

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 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. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including ***Advanced Persistent Threat***, ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible*** 2nd Edition, 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 and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, July 15 - Sat, July 20
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Kevin Fiscus

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.

"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

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

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

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

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

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

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has taught many of SANS most popular classes including SEC401, SEC504, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 505

Securing Windows and Resisting Malware

Six-Day Program • Mon, July 15 - Sat, July 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Fossen

New Course!

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 is the best training so far that I have received. Jason Fossen is the best and most knowledgeable Microsoft geek I have met."
-Ceferino Aratea, Jr. NAVAIR

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 follow along on your laptop. 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).

"You will know and be confident on how to enable Windows PK1 after taking this course. I had no practical experience, but plenty of theory. Jason broke down the pros and cons of the whole process. Excellent!!"
-Othello Swanston, DTRA-DOD

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

"All Windows administrators responsible for securing IIS should attend this course."
-Billy Taylor,
Naval Sea Logistics Center

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

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.

www.giac.org

www.sans.edu

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 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**

"SEC505 teaches you how to use features in Windows that are free, and do the same as the features we're already paying a lot of attention to."
-Magne Smedsrud, NATO

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, July 15 - Sat, July 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Kevin Johnson

Assess Your Web Apps in Depth

"Without a doubt, this was the best class for my career."
-Don Brown, Lockheed Martin

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate to advanced level class, you'll learn the art of exploiting web applications so you can find flaws in your enterprise's web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's web applications to find some of the most common and damaging Web application vulnerabilities today.

Who Should Attend:

- General security practitioners
- Penetration testers
- Ethical hackers
- Website designers and architects
- Developers

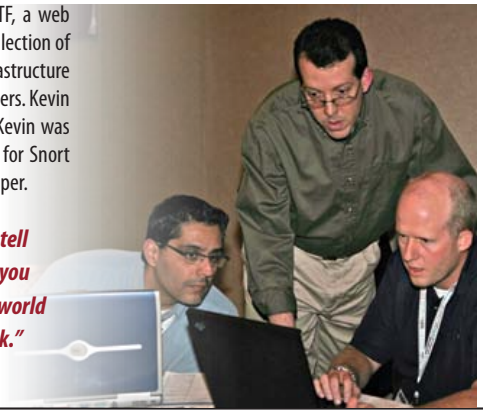
By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, i2P LLC

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

Kevin Johnson *SANS Senior Instructor*

Kevin Johnson is a Senior Security Consultant with Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture, and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises, and penetration testing everything from government agencies to Fortune 100 companies. Kevin is an instructor and author for the SANS Institute and a contributing blogger at TheMobilityHub. Kevin has performed a large number of trainings, briefings, and presentations for both public events and internal trainings. Kevin teaches for the SANS Institute on a number of subjects. He is the author of three classes- SEC542: Web Application Penetration Testing and Ethical Hacking, SEC642: Advanced Web Application Penetration Testing, and SEC571: Mobile Device Security. Kevin has presented at a large number of conventions, meetings, and industry events. Some examples of these are: DerbyCon, ShmooCon, DEFCON, Blackhat, ISACA, Infragard, and ISSA. In addition, Kevin is very involved in the open source community and runs a number of open source projects. These include SamuraiWTF, a web pen-testing environment; Laudanum, a collection of injectable web payloads; Yokoso!, an infrastructure fingerprinting project; and a number of others. Kevin is also involved in MobiSec and SH5ARK. Kevin was the founder and lead of the BASE project for Snort before transitioning that to another developer.



"Fun while you learn! Just don't tell your manager. Every class gives you invaluable information from real-world testing you cannot find in a book."
-David Fava, The Boeing Company

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, July 15 - Fri, July 19
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

Who Should Attend:

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense 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

SPECIAL NOTE: This in-depth course has been updated to incorporate new attack vectors published in version 4.0 of Critical Controls released November 5, 2012. **www.sans.org/critical-security-controls**

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

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

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organization in order to improve its cyber defense."

"This class is extremely valuable for any organization wanting to know where they stand on security."
-David Obrien, Costco

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. Specifically, by the end of the course students will know how to:

- Create a strategy to successfully defend their data
- Implement controls to prevent data from being compromised
- Audit systems to ensure compliance with Critical Control standards.

The course shows security professionals how to implement the controls in an existing network though cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

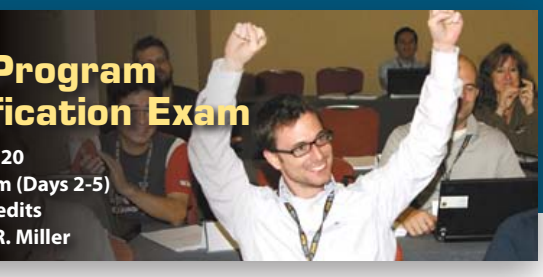
"The course provides a good framework for how to implement the Top 20 controls in a systematic way."
-Mike Schaub, Constellation Energy Nuclear Group

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 performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

MANAGEMENT 414

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



Six-Day Program • Mon, July 15 - Sat, July 20
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: David R. Miller

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

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

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

Obtaining your CISSP® certification consists of:

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

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

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

Who Should Attend:

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

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

David R. Miller *SANS Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on the topics of information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including policy writing, network architecture design to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures (PKI), security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He performs as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, Security Information and Event Management (SIEM) systems, Intrusion Detection and Protection Systems (IDS / IPS), endpoint protection systems, patch management systems, configuration monitoring systems, enterprise data encryption for data at rest, in transit, in use, and within email systems, to describe a few. He regularly performs as a Microsoft Subject Matter Expert (SME) on product lines including Microsoft Server 2008, Exchange Server 2007, Windows 7, and Windows Vista. He has recently been invited by Microsoft Press to assist with the development of Windows Server 8 operating system training and certification materials. David has written curriculum and performed instruction for computer based training videos on Microsoft Windows Server 2008 and IT security courses such as CISSP, SSCP, Security+, CWSP, Data Loss Prevention (DLP), Information Rights Management (IRM), and digital watermarking. David has lectured on network engineering and information systems security to prestigious groups including The Smithsonian Institute, the US Military Academy at West Point, the US Army Advanced Battle Command, the US Department of the Interior, Cisco Systems, Inc., Oracle Corporation, and JP Morgan Chase & Co. Global Financial Services. David is an author, a lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

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

GIAC INFORMATION SECURITY PROFESSIONAL
GISP
www.giac.org

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, July 15 - Fri, July 19
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course 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 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 U.S. government managers and supporting contractors.

Who Should Attend:

- All newly appointed information security officers
- Technically skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who 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, and 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.

"Tremendously valuable experience!! Learned a lot and also validated a lot of our current pratices. Thank you!!"
-Chad Gray, Booz Allen Hamilton

"Every IT security professional should attend no matter what their position. This information is important to everyone."
-John Flood, NASA

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute (**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 (**www.sans.edu/research/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/rocky-mountain-2013**.

www.giac.org

www.sans.edu

AUDIT 507

Auditing Networks, Perimeters, and Systems

Six-Day Program • Mon, July 15 - Sat, July 20
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dave Shackleford

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

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

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

Who Should Attend:

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

"This course is full of relevant, timely, current content, delivered in a highly engaging style. This course is a must for IT auditors and security specialists."

-Brooks Adams, Georgia Southern University

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows 7 Professional 64 bit or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

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

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

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

Dave Shackleford *SANS Senior Instructor*

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

www.giac.org

www.sans.edu

HOSTED

Securing Information Systems Before and After an Incident

One-Day Course | Sun, July 14 | 9:00am - 5:00pm | 6 CPE/CMU Credits | Instructor: Doug Leece

The tongue in cheek title alludes to the facts that legacy systems seldom disappear overnight, technology choices consolidate and expand in a cyclic nature and regulatory influence is increasing along with the capabilities of those attacking the systems. The net result is often a collection of workarounds that have implications on the CIA triad elements.

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

Securing information systems requires an understanding of the current and evolving threat landscape as well as foundational knowledge of network technology and system designs often encountered in organizations. This course will combine lecture, demo and interactive exercises that examine how to overlay threat knowledge and governance requirements onto the I.T. systems as they are presently implemented, then determine gaps and realistic options for security protection, system monitoring and incident response.

Starting with a focus on the most common technology stack and architectural solutions followed by market and regulatory pressures, the landscape a security professional is likely to be protecting is defined. Developing a defendable security program also requires credible knowledge about threats faced by the organization both externally and internally, whether it's hacktivism or mobile devices. Current tools and techniques used to attack applications and the underlying systems will be discussed and demonstrated during this class, as well as providing guidance on threat modeling that can be used back at the office.

Existing security control technology categories from file integrity to web application and between will be examined at both the capability and deployment consideration level. Guidance around implementing operational security activities like vulnerability management and event monitoring is another key element to this one day course. The day will finish with details about current and leading digital forensic practices and designing information system security to support a forensic investigation in the event it is required.

A True Hands-On Interactive Security Challenge!

NetWars is a computer and network security challenge designed to test participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals.

- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing
- Intrusion Detection

The NetWars competition will be played over two evenings: July 18-19, 2013. Prizes will be awarded at the conclusion of the games. REGISTRATION IS LIMITED AND IS FREE to students attending any long course at SANS Rocky Mountain 2013 *(NON-STUDENTS ENTRANCE FEE IS $1,095)*.

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

Bonus Sessions

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given by our instructors and selected subject matter experts help you broaden your knowledge, hear from the voices that in matter in computer security, and get the most for your training dollar.

Keynote: Windows Exploratory Surgery *Jason Fossen*

In this talk we'll rummage around inside the guts of Windows while on the lookout for APT malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware.

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.

CISSP: The Good, The Bad, and Why You Need It *David R. Miller*

Being one of the most sought after certifications by hiring companies and the government, it is also one of the more difficult to achieve by the job seekers. This certification requires a broad and comprehensive overview of how an enterprise would begin to implement a security structure in the enterprise, and then maintain it to protect the safety of people and the security of the valuable information assets. It involves the senior management team and the end users, and everything in between. It balances technology with security concepts and requires a clear vision of both. Whether you need the certification to get that job or promotion or the raise youve been after, or you desire to improve your professional skills in your pursuit of increased individual performance and capability, this body of knowledge will provide you with both. The vision of the enterprise you will develop during this course will surprise you, and many aspects will directly apply outside the enterprise in your daily life.

OODA - The Secret to Effective Security in Any Environment *Kevin Fiscus*

OODA, or Observe, Orient, Decide, and Act is a concept first developed for fighter pilots. The concept states that the adversary who can effectively complete the OODA cycle first will go home while the adversary who takes longer enjoys, at best, a long, slow parachute ride to the ground. This concept can, and perhaps should, be applied to information security. In theory, we defenders should have the advantage as it is our "house" the attackers are attacking. Unfortunately, that is rarely the case. All too often defenders don't even start their OODA loop until after the attacker has completed the compromise. Fortunately, there are some simple steps we can take to regain the advantage.

Information Assurance 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 how do you integrate information assurance metrics in an organization and 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.

Sharing Without Borders: Attacking and Testing SharePoint *Kevin Johnson*

In this talk, Kevin Johnson of Secure Ideas will examine SharePoint, how it works, and the common flaws it exposes within an organization. Kevin will also discuss some tricks and tips on how to assess the system, including exploits and attacks a penetration tester can use against SharePoint.

GIAC Program Overview *Stephen Northcutt*

SANS Technology Institute Open House *Stephen Northcutt*

For dates, times, and complete information, visit www.sans.org/event/rocky-mountain-2013/bonus-sessions

Vendor Showcase

Tuesday, July 16 | 10:30am-10:50am • 12:30pm-1:15pm • 3:00pm-3:20pm

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

What's Your Next Career Move?

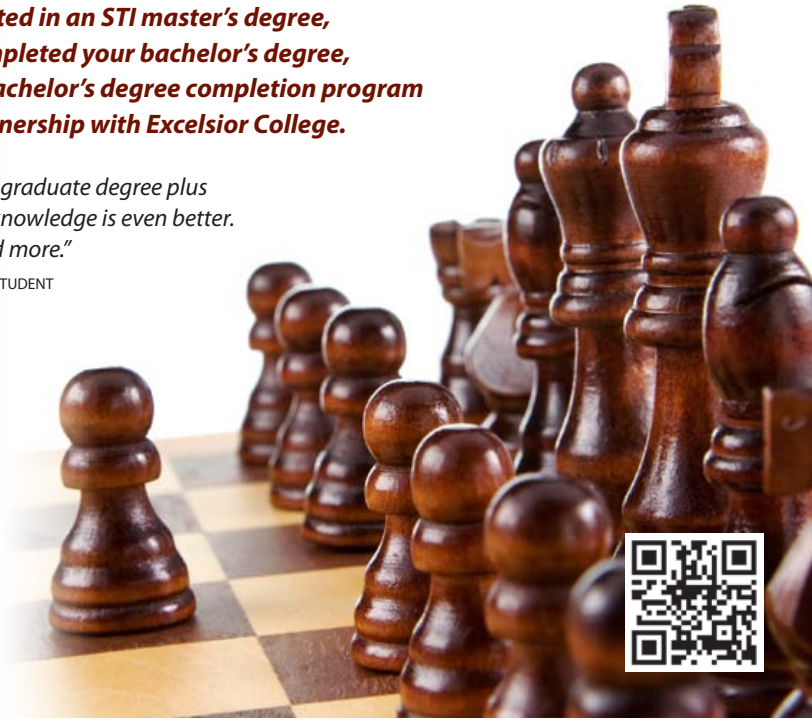
The SANS Technology Institute (STI) offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

If you are interested in an STI master's degree, but have not completed your bachelor's degree, we now offer a bachelor's degree completion program through our partnership with Excelsior College.

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



SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu

How Are You Protecting Your

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

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

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

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Get Certified at
www.giac.org

Future SANS Training Events

SANS **Security West** 2013

San Diego, CA
May 7-16, 2013
www.sans.org/event/security-west-2013

SANS **Austin** 2013

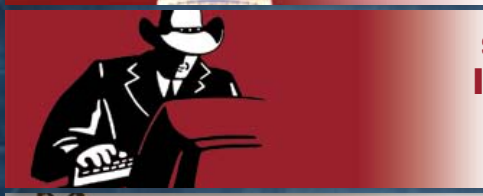
Austin, TX
May 19-24, 2013
www.sans.org/event/austin-2013

SANS **Mobile Device Security** SUMMIT

Southern California | May 30 - June 6, 2013
www.sans.org/event/mobile-device-security-summit-2013

SANSFIRE 2013

Washington, DC
June 15-22, 2013
www.sans.org/event/sansfire-2013



SANS **Digital Forensics & Incident Response** SUMMIT

Austin, TX | July 9-16, 2013
www.sans.org/event/dfir-summit-2013

SANS **San Francisco** 2013

San Francisco, CA
July 29 - August 3, 2013
www.sans.org/event/san-francisco-2013

SANS **Boston** 2013

Boston, MA
August 5-10, 2013
www.sans.org/event/boston-2013

SANS **Virginia Beach** 2013

Virginia Beach, VA
August 19-30, 2013
www.sans.org/event/virginia-beach-2013

SANS **Capital City** 2013

Washington, DC
September 3-8, 2013
www.sans.org/event/capital-city-2013

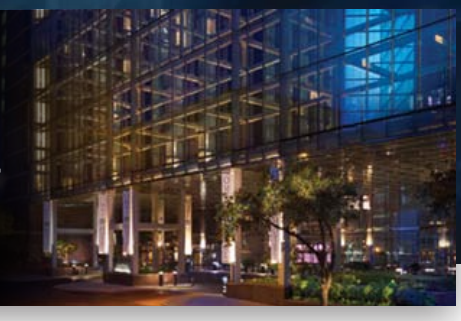
SANS **Network Security** 2013

Las Vegas, NV
September 14-23, 2013
www.sans.org/event/network-security-2013

Dates may change. Get the complete list of events at www.sans.org

SANS Rocky Mountain 2013

Hotel Information



Conference Location
Hyatt Regency Denver Convention Center

650 15th Street | Denver, CO 80202
Phone: 303-436-1234
denverregency.hyatt.com

Special Hotel Rates Available

A special discounted rate of $194.00 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 June 23, 2013. To make reservations please call (800) 233-1234 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.

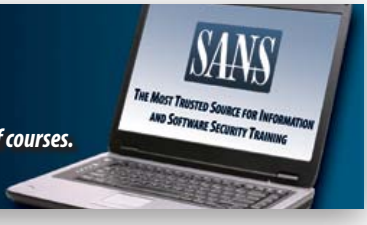
The hotel will require a major credit card to guarantee your reservation. To cancel your reservation, you must notify the hotel at least 72 hours before your planned arrival date.

Top 5 reasons to stay at the Hyatt Regency Denver Convention Center

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 Hyatt Regency Denver Convention Center, 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 Hyatt Regency Denver Convention Center that you won't want to miss!
5. Everything is in one convenient location!

SANS Rocky Mountain 2013

Registration Information



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

To register, go to www.sans.org/event/rocky-mountain-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 June 19, 2013 – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**5/29/13**	**$500.00**	**6/12/13**	**$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 Voucher Discount Program pays you credits and delivers flexibility.

www.sans.org/vouchers