SANS Atlanta 2016

Atlanta, GA April 4-9

Choose from these popular courses:

NEW! **Network Penetration Testing and Ethical Hacking**

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits. and Incident Handling

Intrusion Detection In-Depth

Windows Forensic Analysis

SANS Training Program for CISSP® Certification

THE MOST TRUSTED SOURCE

FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

"SANS courses give you the knowledge to think like an attacker and as such better equip you to defend your networks."

-Sheryll Tiauzon, Coca-Cola Company

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

SAVE $400

by registering and paying early!

See page 13 for more details.

sans.org/atlanta-2016

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to become SANS instructors. This guarantees that what you learn in class will be up-to-date and relevant to your job. The SANS Atlanta 2016 line-up of instructors includes:

Ovie Carroll
Certified Instructor

Jonathan Ham
Certified Instructor

David R. Miller
Instructor

Chris Pizor
Instructor

Dave Shackleford
Senior Instructor

Bryan Simon
Certified Instructor

Evening Bonus Sessions

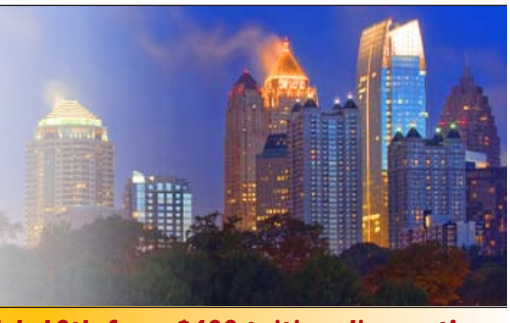
Take advantage of these extra evening presentations and add more value to your training. Learn more on page 8.

Continuous Ownage: Why you Need Continuous Monitoring
Bryan Simon

The CISSP® Exam was Implemented on April 15, 2015
David Miller

The training campus for SANS Atlanta 2016, Crowne Plaza Atlanta Midtown, is located between Downtown Atlanta and Buckhead. The Crowne Plaza Atlanta Midtown is the perfect hotel to fulfill both relaxation and business needs.

PAGE 13



Be sure to register and pay by Feb 10th for a $400 tuition discount!

Courses-at-a-Glance

The Value of SANS Training & YOU

EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. 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 really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need 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 learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

"Bryan is by far the best instructor and he kept the class interesting and all students engaged. Best training I have ever attended – SANS lived up to it's reputation."
-Ryan O'Connor, Atlantic Health

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, he has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 11 GIAC certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jonathan Ham
- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Who Should Attend

- Intrusion detection analysts (all levels)
- Network engineers
- System, security, and network administrators
- Hands-on security managers

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"The threats to our businesses and government agencies are ever increasing. We need to focus our IDS/IPS on our critical data and SEC503 helps us achieve that."
-Ed Brewster, SAIC, Inc.

"SEC503 covers the best processes for intrusion analysis, how to cut out most of the network noise, and identify the important traffic."
-Mike Boya, Warner Bros.

Jonathan Ham *SANS Certified Instructor*

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Chris Pizor

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), 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. As defenders, it is essential we understand these hacking tools and techniques.

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

"SEC504 was very structured, well-presented, interesting, and engaging for people new to the field as well as experienced professionals."
-Ewa Konkolska, Prudential Insurance

"SEC504 is the best security and IT course, in my opinion, and every security professional should take it."
-Samir Hassan, eHealth Ontario

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, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. This will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. 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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

Chris Pizor *SANS Instructor*

Chris Pizor is a civilian employee working for the U.S. Air Force as the lead curriculum designer for cyber warfare operations training. Chris served on active duty in the USAF as a Network Intelligence Analyst before retiring in 2010. He was part of the initial cadre of the NSA Threat Operations Center and helped developed tactics to discover and eradicate intrusions into U.S. government systems. Chris has worked for 20 years in the Intelligence Community, including 12 years focused on cybersecurity. Over the course of his active duty career, Chris received multiple individual and team awards. Chris is passionate about security and helping others advance their security knowledge. He is continuously researching and refining his own skills so he can prepare U.S. airman and other professionals to defend their vital networks and critical infrastructure. Chris earned a Bachelor's Degree in Intelligence Studies and Information Operations, and is actively pursuing a Master's Degree in Cybersecurity. He holds the GSEC, GCIA, GCIH, GPEN, GXPN and GCFA certifications. When Chris isn't working, he enjoys spending time with his wife and two young children, woodworking, and spending time outdoors.

SEC560:
Network Penetration Testing and Ethical Hacking

NEW

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Dave Shackleford

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 is the must-have course for every well-rounded security professional.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently…and masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

giac.org

sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

"SEC560 has helped me have a more in-depth knowledge of penetration testing. The instructor's flow and method made it easier to understand."
-Mithra Ravendran, BAE Systems Applied Intelligence

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. @daveshackleford

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ovie Carroll

- GIAC Cert: GCFE
- STI Master's Program
- OnDemand Bundle

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

digital-forensics.sans.org

"Awesome content, awesome instructor! Everyone needs this course, not just forensics, but any security personnel."
-Thomas Farley, Raytheon

"I like the fact that the whole course is centered around the same data and that there is so much data available. I can't wait to try this out at work!"
-Greg Dub, National Center for Policy Analysis

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

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

Ovie Carroll *SANS Certified Instructor*

Ovie Carroll has over 20 years of federal law enforcement experience. Ovie was a special agent for the Air Force Office of Special Investigations (AFOSI) and Chief of the Washington Field Office Computer Investigations and Operations Branch responsible for investigating all national-level computer intrusions into USAF computer systems. Following his career with the AFOSI he was the Special Agent in Charge of the Postal Inspector General's computer crimes unit, where he was responsible for all computer intrusion investigations and for providing all computer forensic analysis in support of USPS-OIG investigations. Ovie is currently the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) and an adjunct professor at George Washington University teaching computer crime investigations. In addition to his career fighting computer crime, Ovie has conducted investigations into a variety of offenses including murder, fraud, bribery, theft, gangs and narcotics.

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

"SANS does it again! An excellent course (MGT414) for those looking to lead their companies through the next stage of security evolution."
-Travis Anderson, Pacific Gas and Electric Company

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand 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® 8 domains
- Security professionals and managers looking for practical ways to apply the 8 domains of knowledge to their current activities

You Will Be Able To:

- Understand the 8 domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the 8 domains of knowledge
- Apply the skills learned across the 8 domains to solve security problems when you return to work

giac.org

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
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, and enterprise data encryption for data at rest, in transit, in use, and within email systems, to name a few. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE:

Continuous Ownage: Why you Need Continuous Monitoring

Bryan Simon

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course: SANS SEC511: Continuous Monitoring and Security Operations.

The CISSP® Exam was Implemented on April 15, 2015

David Miller

Are you interested in the CISSP certification? How might it improve your career? On the resume? Getting a new job? On the business card? Maintaining your career and moving you up the ladder. With your skill set? As the professional you are. How about helping with that pay raise? We will look at how management views this well sought-after certification. Have you been studying for it? Do you plan to take the exam real soon? On January 15, 2015 ISC^2, the certifying body for the CISSP certification exam, released a new set of exam objectives for the CISSP certification exam. These changes were implemented on the CISSP certification exam beginning April 15, 2015. This new set of exam objectives is a major change from the previous version of the CISSP exam. ISC^2 has moved and merged content to form 8 Domains of the Common Body of Knowledge, down from 10 Domains in the previous exam. They have also added numerous new topics to the objectives. You will need to know about the new material you will be tested on. Learn the new shape and the new topics of the 2015 CISSP Certification exam.

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & **GIAC Certification Attempt**

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers
sans.org/security-training/by-location/all

Community SANS
Live Training in Your Local Region with Smaller Class Sizes
sans.org/community

Private Training
Your Location! Your Schedule!
sans.org/private-training

Mentor
Live Multi-Week Training with a Mentor
sans.org/mentor

Summit
Live IT Security Summits and Training
sans.org/summit

ONLINE TRAINING

OnDemand
E-learning Available Anytime, Anywhere, at Your Own Pace
sans.org/ondemand

vLive
Online, Evening Courses with SANS' Top Instructors
sans.org/vlive

Simulcast
Attend a SANS Training Event without Leaving Home
sans.org/simulcast

OnDemand Bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning sans.org/ondemand/bundles

FUTURE SANS TRAINING EVENTS

Security East 2016
New Orleans, LA | Jan 25-30

Cyber Threat Intelligence SUMMIT & TRAINING 2016
Alexandria, VA | Feb 3-10

Scottsdale 2016
Scottsdale, AZ | Feb 8-13

McLean 2016
McLean, VA | Feb 15-20

ICS Security
SUMMIT & TRAINING 2016
Orlando, FL | Feb 16-23

Anaheim 2016
Anaheim, CA | Feb 22-27

Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

SANS **Reston** 2016
Reston, VA | Apr 4-9

Threat Hunting and Incident Response
SUMMIT & TRAINING 2016
New Orleans, LA | Apr 12-19

Pen Test Austin 2016
Austin, TX | Apr 18-23

Security West 2016
San Diego, CA | April 29 - May 6

Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

Security Operations Center
SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

SANSFIRE 2016
Washington, DC | June 11-18

Information on all events can be found at
sans.org/security-training/by-location/all

SANS ATLANTA 2016

Hotel Information

Training Campus
Crowne Plaza Atlanta Midtown

590 West Peachtree Street
Atlanta, GA 30308
855-646-8549
sans.org/event/atlanta-2016/location

Located between Downtown Atlanta and Buckhead, the Crowne Plaza Atlanta Midtown is the perfect hotel to fulfill both relaxation and business needs. The spacious, modern rooms have unbeatable views and offer free Wi-Fi Internet.

Special Hotel Rates Available

A special discounted rate of $149.00 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 March 18, 2016.

Top 5 reasons to stay at the Crowne Plaza Atlanta Midtown

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 Crowne Plaza Atlanta Midtown 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 Crowne Plaza Atlanta Midtown that you won't want to miss!
5. Everything is in one convenient location!

SANS ATLANTA 2016

Registration Information

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

Register online at sans.org/atlanta-2016/courses

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

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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-10-16**	**$400.00**	**3-2-16**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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 March 16, 2016 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers