SANS

The Most Trusted Source for Information Security Training, Certification, and Research

ROCKY MOUNTAIN FALL 2017

Denver, CO | September 25-30

Protect Your Business and Advance Your Career

Five hands-on, immersion-style information security courses taught by real-world practitioners

CYBER DEFENSE
ETHICAL HACKING
DIGITAL FORENSICS
MANAGEMENT

GIAC CERTIFICATIONS

"SANS training is always relevant and provides up-to-date information that spurs ideas on how to better implement security in our environment."
-Dan Smith, Raytheon Company

SAVE $400

Register and pay by Aug 2nd – Use code **EarlyBird17**

www.sans.org/rocky-mountain-fall

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 teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Rocky Mountain Fall 2017 lineup of instructors includes:

Sergio Caltagirone
Instructor
@cnoanalysis

Christopher Crowley
Principal Instructor
@CCrowMontance

Matt Edmondson
Instructor
@matt0177

Randy Marchany
Certified Instructor
@randymarchany

Dave Shackleford
Senior Instructor
@daveshackleford

Jake Williams
Certified Instructor
@MalwareJake

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 7.

KEYNOTE: ***Infosec State of the Union*** – Jake Williams

State of the Dark Web – Matt Edmondson

MT6D: Moving Target IPv6 Defense – Randy Marchany

The training campus for SANS Rocky Mountain Fall 2017 is the Grand Hyatt Denver. The hotel is located near the 16th Street Mall, a prime setting just moments from the most popular attractions in the city.

PAGE 13

Save $400 when you register and pay by August 2nd using code EarlyBird17

Courses at a Glance

	MON 9-25	TUE 9-26	WED 9-27	THU 9-28	FRI 9-29	SAT 9-30
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	Page 4					
FOR578 Cyber Threat Intelligence	Page 5					
MGT517 Managing Security Operations: Detection, Response, and Intelligence	Page 6 *NEW!*					

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Dave Shackleford

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 specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

"This course has opened my eyes to just how important security is, and has given me a deeper understanding of how to protect our systems."

-Travis Sorensen, Xpress Solutions

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our 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 rise in advanced persistent threats, 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 will 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.

SANS Technology Institute
www.sans.edu


www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

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**

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Matt Edmondson

Who Should Attend

- Incident handlers
- 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 content is up-to-date. The labs are awesome and they work! The material is just right for a mid-level course."
-Dan Eckstein, Nationwide

"I especially enjoyed how Matt included his personal experiences to reinforce the course content."
-Dan McClain, Regions Financial Corp.

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.**

"Fills the gap of 'here's what adversaries do and the evidence it leaves.'"
-Kevin Heithaus, JPMorgan Chase

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 for, detect, and respond to those attacks. 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, exploiting, and defending systems. **This course 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.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Matt Edmondson *SANS Instructor*

Matt performs technical duties for the U.S. government and is a principal at Argelius Labs, where he performs security assessments and consulting work. Matt's extensive experience with digital forensics includes conducting numerous examinations and testifying as an expert witness on multiple occasions. A recognized expert in his field with a knack for communicating complicated technical issues to non-technical personnel, Matt routinely provides cybersecurity instruction to individuals from the Department of Defense, Department of Justice, Department of Homeland Security, Department of the Interior, as well as other agencies, and has spoken frequently at information security conferences and meetings. Matt is a member of the SANS Advisory Board and holds 11 GIAC certifications, including the GREM, GCFA, GPEN, GCIH, GWAPT, GMOB and GCIA. In addition, Matt holds the Offensive Security Certified Professional (OSCP) certification. **@matt0177**

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

GCCC Certification
Critical Controls

www.giac.org/gccc

Five-Day Program
Mon, Sep 25 - Fri, Sep 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Randy Marchany

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- 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
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

"This training gets right to the point quickly, and the labs are very clear and concise."

-Duane Harper, Community Health Systems

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Cybersecurity attacks are increasing and evolving so rapidly that it 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? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

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 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.

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 organisation in order to improve its cyber defence."

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.

The course shows security professionals how to implement the Controls in an existing network through 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.

Randy Marchany *SANS Certified Instructor*

Randy is the Chief Information Security Officer of at Virginia Tech University and the Director of Virginia Tech's IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. Randy is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks of 2000. **@randymarchany**

FOR578

Cyber Threat Intelligence

GIAC Certification Available Late 2017

Five-Day Program
Mon, Sep 25 - Fri, Sep 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructors: Jake Williams, Sergio Caltagirone

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR500 (formerly FOR408), FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

"Absolutely loved this class!"

-Nate DeWitt, eBay, Inc.

▶II **Bundle OnDemand**
WITH THIS COURSE
www.sans.org/ondemand

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- **Understand and develop skills in tactical, operational, and strategic-level threat intelligence**
- **Generate threat intelligence to detect, respond to, and defeat advanced persistent threats**
- **Validate information received from other organizations to minimize resource expenditures on bad intelligence**
- **Leverage open-source intelligence to complement a security team of any size**
- **Create Indicators of Compromise in formats such as YARA, OpenIOC, and STIX**

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

Jake Williams *SANS Certified Instructor*

Jake Williams is a principal consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. He is well versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation. Jake developed Dropsmack, a pentesting tool (okay, malware) that performs command and control and data exfiltration over cloud file sharing services. Jake also developed an anti-forensics tool for memory forensics, Attention Deficit Disorder (ADD). This tool demonstrated weaknesses in memory forensics techniques. **@MalwareJake**

Sergio Caltagirone *SANS Instructor*

Sergio Caltagirone hunts evil. He spends days hunting hackers and evenings hunting human traffickers. During nine years with the U.S. Department of Defense as a senior threat intelligence analyst and technical director, he hunted the most sophisticated cyber threats in the world. During over three years as Director of Threat Intelligence at Microsoft, he developed and implemented its threat intelligence program protecting billions of customers worldwide. Now as Director of Threat Intelligence and Analytics at Dragos, Sergio safeguards critical infrastructure and industrial control systems. He created the Diamond Model of Intrusion analysis, helping bring more pain to adversaries by strengthening hunters and intelligence analysts. He also serves as the Technical Director of the Global Emancipation Network, a non-profit non-governmental organization, leading a world-class all-volunteer team hunting human traffickers and finding their victims through data science and analytics. **@cnoanalysis**

MGT517

Managing Security Operations: Detection, Response, and Intelligence *NEW!*

Five-Day Program
Mon, Sep 25 - Fri, Sep 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

Who Should Attend

- Information security managers
- SOC managers, analysts, and engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/system administration/ network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

"Chris is a fantastic instructor, has great pacing with engaging anecdotes, and he's very insightful."
-Rich Savacool, Nixon Peabody

This course covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed to have the ability to adjust and work within the context and constraints of an organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment, as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- **Business alignment and ongoing adjustment of capabilities and objectives**
- **Designing the SOC and the associated objectives of functional areas**
- **Software and hardware technology required for performance of functions**
- **Knowledge, skills, and abilities of staff as well as staff hiring and training**
- **Execution of ongoing operations**

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organization.

Course Author Statement

"The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for specialists to look only at their piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a Security Operations Center (SOC) as a tool, and not as the unification of people, processes, and technologies.

"This course provides a comprehensive picture of a Cyber Security Operations Center. Discussion on the technology needed to run a SOC is handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. The course outlines staff roles, addresses staff training through internal training and information-sharing, and examines the interaction between functional areas and data exchange.

"After attending this class, the participant will have a roadmap for what needs to be done in an organization seeking to implement security operations."

-Christopher Crowley

Christopher Crowley *SANS Principal Instructor*

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. **@CCrowMontance**

Bonus Sessions

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: Infosec State of the Union

Jake Williams

Come attend this session and catch up with the latest InfoSec news and how it impacts your organization. We'll talk about Russian election hacking, FBI investigative techniques, implications of the latest Shadow Brokers dumps, software product liability, the Department of Justice protecting government exploits and more. Come hang with us for this session, and you'll walk away bigger, badder, and smarter.

State of the Dark Web

Matt Edmondson

Have you heard people talk about the dark web for the past few years and wondered what all the fuss was about? Maybe you've even fired up TOR and visited an .onion site or two for "research." Well if you want to take your dark web knowledge from moderate to cromulent, this is the presentation for you! We'll cover deep web vs. dark web, how big the dark web really is, what's on there, how you find content and a few cool things you can do. We may even have time to show a few other dark webs.

MT6D: Moving Target IPv6 Defense

Randy Marchany

This talk explains how MT6D works and how similar defense schemes can help reduce target visibility. We'll also show a demo of the system at work.Virginia Tech University has been running a full production dual stack IPv4/IPv6 network since 2005. This has allowed the IT Security Office and Lab to develop some unique DDOS defense mechanisms for IPv6. MT6D is conceptually identical to radio frequency hopping, but jumps IP addresses instead of radio frequencies. Session information is maintained as the two hosts jump to new addresses within the Virginia Tech IPv6 subnets. One of our v6 subnets contains 10**19 addresses (IPv4's total address space is ~10**10 addresses), so the probability of address collision is very low. The size of these v6 subnets makes it difficult for attackers to use traditional network scanning techniques to find a target. An MT6D session works by having the sender and receiver jump to new IPv6 addresses at a predetermined interval (for example, every two seconds), which makes it difficult for an attacker to DDOS either host.

SANS SECURITY AWARENESS

Security Awareness Training by the Most Trusted Source

Protect Your Employees

Keep your organization safe with flexible computer-based training.

End User
CIP
ICS Engineers
Developers
Healthcare

- Train employees on their own schedule
- Modify modules to address specific audiences
- Increase comprehension – courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes

Learn more about SANS Security Awareness at:

securingthehuman.sans.org

Enhance Your Training Experience

Add an
OnDemand Bundle & GIAC Certification Attempt* to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an 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.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- 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.

The best. Made better.

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive and rigorous graduate education experience.

"Joining the SANS Master's Program was probably one of the best decisions I've ever made."

– John Hally, MSISE, EBSCO Information Services

SANS Technology Institute

Begin your first course in Denver this fall!

MASTER OF SCIENCE DEGREES

- Information Security Engineering: MSISE
- Information Security Management: MSISM

GRADUATE CERTIFICATE PROGRAMS

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

GIAC CERTIFICATIONS

Students earn industry-recognized GIAC certifications during most technical courses.

Funding for Veterans

Master's degree and graduate certificate programs are eligible for VA Education Benefits.

Corporate Tuition Reimbursement

SANS Technology Institute is regionally accredited by the Middle States Commission on Higher Education, so tuition is eligible for most corporate tuition reimbursement plans.

www.sans.edu | info@sans.edu

The SANS Technology Institute is accredited by The Middle States Commission on Higher Education (3624 Market Street, Philadelphia, PA 19104 – 267-284-5000), an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government Web site at: www.benefits.va.gov/gibill

SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS' training events feature SANS' top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 12 for upcoming training events in North America.

Summits

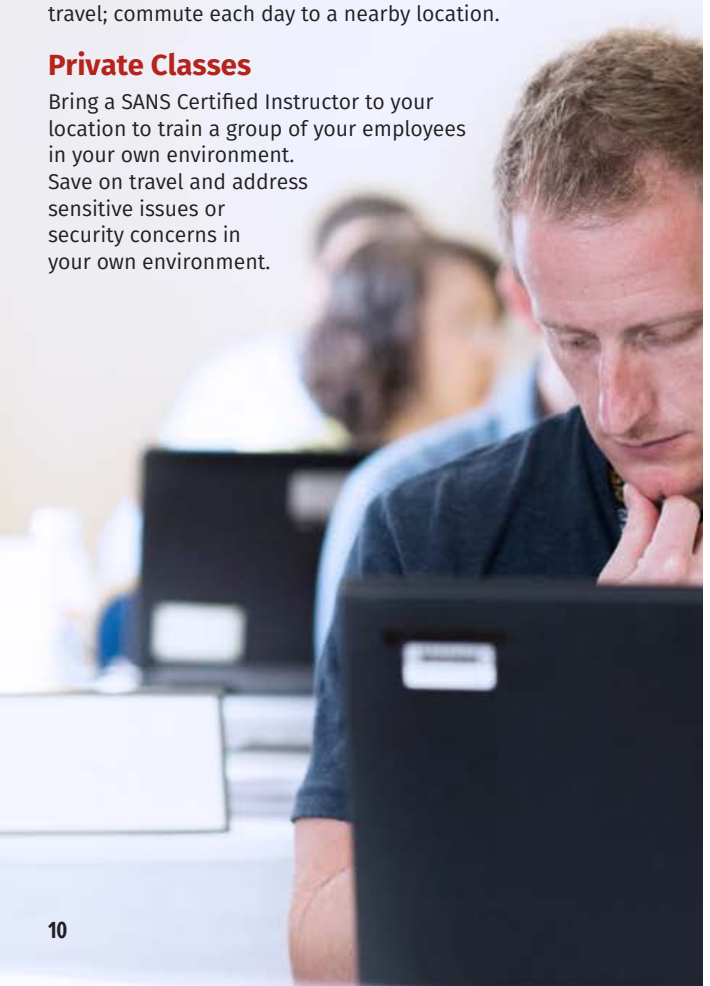
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certifications each year.

Top reasons to take SANS courses online:

- **Learn at your own pace, over four months**
- **Spend extra time on complex topics**
- **Repeat labs to ensure proficiency with skills**
- **Save on travel costs**
- **Study at home or in your office**

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

> **"I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time."**
>
> -Kevin E., U.S. Army

> **"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."**
>
> -Dan Trueman, Novae PLC

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or sponsoring an academy to meet your specific talent needs.

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

SANS | CyberTalent
IMMERSION ACADEMY

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

Future Training Events

SANSFIRE — Washington, DC — July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security — Las Vegas, NV — Sep 10-17

Baltimore Fall	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9

Cyber Defense Initiative — Washington, DC — Dec 12-19

Future Summit Events

ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Grand Hyatt Denver
1750 Welton Street
Denver, CO 80202
Phone: 303-295-1234
www.sans.org/event/rocky-mountain-fall-2017/location

The Grand Hyatt Denver is located near the 16th Street Mall, a prime setting just moments from the most popular attractions in the city. Discover what happens when urban luxury meets personalized service and enjoy instant access to everything the vibrant city of Denver has to offer.

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through **September 1, 2017**.

Top 5 reasons to stay at the Grand Hyatt Denver

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

Registration Information

Register online at **www.sans.org/rocky-mountain-fall**

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

Select your course 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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**8-2-17**	**$400.00**	**8-23-17**	**$200.00**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **September 6, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

Open a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account