THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS

Rocky Mountain 2017

Denver, CO | June 12-17

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

10 courses in:

CYBER DEFENSE
DETECTION & MONITORING
PENETRATION TESTING
INCIDENT RESPONSE
CYBER THREAT INTELLIGENCE
DIGITAL FORENSICS
ETHICAL HACKING
MANAGEMENT
ICS/SCADA SECURITY

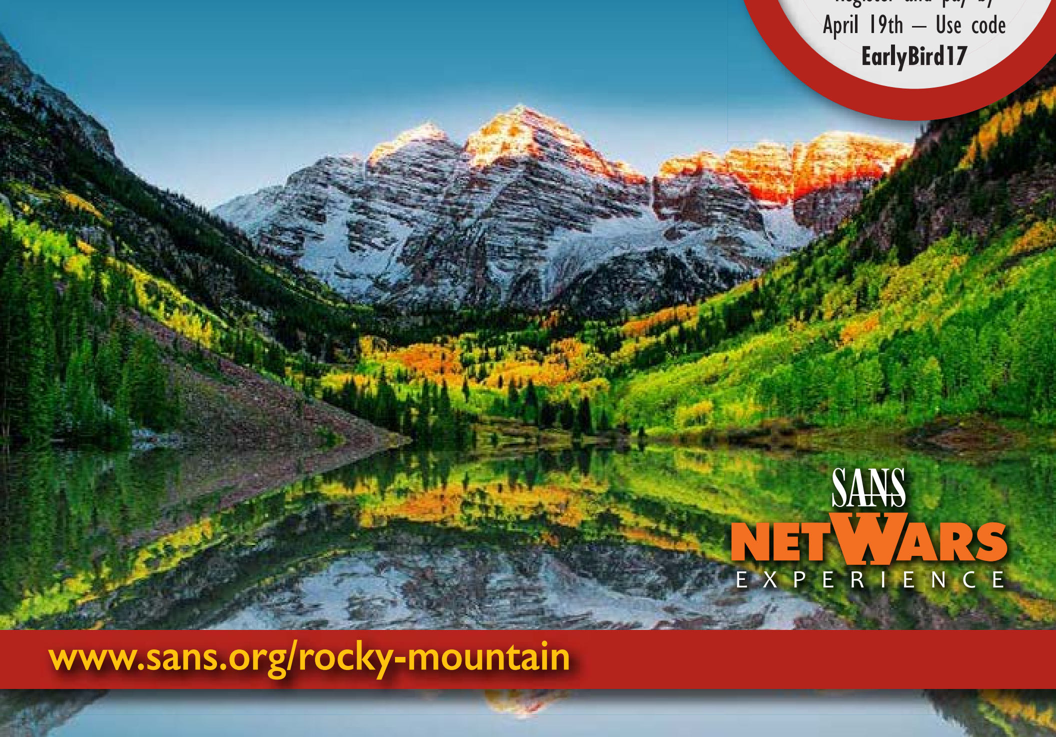
GIAC CERTIFICATIONS

GIAC-Approved Training

"SANS training is extremely valuable for use in the real world, and I'm amazed at the depth of information provided."
-J. Aiken, BASF

SAVE $400

Register and pay by April 19th – Use code **EarlyBird17**



SANS NETWARS EXPERIENCE

www.sans.org/rocky-mountain

SANS Rocky Mountain 2017

DENVER, CO
JUNE 12-17

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 2017 lineup of instructors includes:

Eric Conrad
Senior Instructor
@eric_conrad

Adrien de Beaupre
Certified Instructor
@adriendb

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Bryce Galbraith
Principal Instructor
@brycegalbraith

G. Mark Hardy
Certified Instructor
@g_mark

Micah Hoffman
Certified Instructor
@WebBreacher

Rob Lee
Faculty Fellow
@robtlee
@sansforensics

Keith Palmgren
Senior Instructor
@kpalmgren

Billy Rios
Instructor
@XSSniper

Scott Roberts
Instructor
@sroberts

Evening Bonus Sessions

Take advantage of these extra evening presentations
and add more value to your training. Learn more on page 12.

KEYNOTE: ***Welcome Threat Hunters, Phishermen, and Other Liars*** – Rob Lee

Quality Not Quantity: Continuous Monitoring's Deadliest Events – Eric Conrad

Anti-Ransomware: How to Turn the Tables – G. Mark Hardy

So, You Wanna Be a Pentester? – Adrien de Beaupre

Collecting and Exploiting Your "Private" Internet Data Using OSINT – Micah Hoffman

Internet of Things (IoT) and Embedded Device Security Research – A Primer – Billy Rios

Save $400 when you register and pay by April 19th using code EarlyBird17

Courses at a Glance

<table>
<tr><th></th><th></th><th>MON 6-12</th><th>TUE 6-13</th><th>WED 6-14</th><th>THU 6-15</th><th>FRI 6-16</th><th>SAT 6-17</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security</td><td colspan="5">Page 2</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">Page 3 SIMULCAST</td></tr>
<tr><td>SEC511</td><td>Continuous Monitoring and Security Operations</td><td colspan="6">Page 4 SIMULCAST</td></tr>
<tr><td>SEC504</td><td>Hacker Tools, Techniques, Exploits, and Incident Handling</td><td colspan="6">Page 5 SIMULCAST</td></tr>
<tr><td>SEC542</td><td>Web App Penetration Testing and Ethical Hacking</td><td colspan="6">Page 6</td></tr>
<tr><td>SEC560</td><td>Network Penetration Testing and Ethical Hacking</td><td colspan="6">Page 7 SIMULCAST</td></tr>
<tr><td>FOR508</td><td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td><td colspan="6">Page 8</td></tr>
<tr><td>FOR578</td><td>Cyber Threat Intelligence</td><td colspan="5">Page 9</td><td></td></tr>
<tr><td>MGT512</td><td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td><td colspan="5">Page 10</td><td></td></tr>
<tr><td>ICS410</td><td>ICS/SCADA Security Essentials</td><td colspan="5">Page 11</td><td></td></tr>
</table>

Register today for SANS Rocky Mountain 2017!
www.sans.org/rocky-mountain

@SANSInstitute
Join the conversation:
#SANSRocky

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 deliver SANS' top instructors teaching multiple courses at a single time and location, allowing

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interactions and learning from other professionals
- @Night events, NetWars, Vendor presentations, industry receptions, and many other benefits

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 97 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 each year and frequently achieve certification.

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.

> **"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

SEC301: Intro to Information Security

Five-Day Program
Mon, June 12 - Fri, June 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

www.giac.org/gisf

▶❚❚ **Bundle OnDemand** with this course
www.sans.org/ondemand

"Excellent course for someone who is looking to become a security engineer or to improve existing IT security practices."
-Ansar Khalil, HomeStreet Bank

"Keith is very engaging and he not only helped me greatly to understand the topics, but also made them interesting to learn."
-Jennifer Bakowski, John Hancock Financial Services

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge but are new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Intro to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Authored by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

"Keith is an educational genius to have me grasping HEX and BIN in twenty minutes!"
-Lisa Bruere, LMI Aerospace Inc.

Keith Palmgren *SANS Senior Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice, responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SEC401:

Security Essentials Bootcamp Style

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryce Galbraith

Also Available via Simulcast

See page 17 for details.

www.giac.org/gsec

www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"Bryce has excellent knowledge and passion for security and this shows in his delivery of the material."
-Ron Austin,
Sony Network Entertainment

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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*!

With the rise of 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'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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the international bestseller *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. He has held security positions at global ISPs and Fortune 500 companies, was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences worldwide. @brycegalbraith

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/rocky-mountain-2017/courses

SEC511:

Continuous Monitoring and Security Operations

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Eric Conrad

ALSO AVAILABLE VIA SIMULCAST

See page 17 for details.

GMON

www.giac.org/gmon

SANS Technology Institute

www.sans.edu

▶❚❚ BUNDLE ONDEMAND WITH THIS COURSE

www.sans.org/ondemand

"This training provides excellent information for self assessment of current SEC practices. I picked up a lot of tricks and new perspectives."
-Kyle Montgomery, National Rural Electric Cooperative Association

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)
- Computer Network Defense analysts

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

"Eric has great energy and knowledge, which keeps everyone interested and awake!"
-Daniel Moy, Adobe

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

"This course is full of practical and actionable advice for environments of any size."
-Jesse Lane, IAG

Eric Conrad *SANS Senior Instructor*

Eric Conrad is lead author of the book *The CISSP Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. @eric_conrad

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

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
- 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

"If you love cybersecurity and learning how exploits work, you NEED this course!"
-Jaid, U.S. Navy

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 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 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.**

"Adrien is an awesome instructor, very knowledgeable, and relates information in common terms to the skill-sets I'm trying to acquire."
-Bill D., U.S. Army

ALSO AVAILABLE VIA SIMULCAST
See page 17 for details.

GCIH
www.giac.org/gcih

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

▶❚❚
Bundle OnDemand
with this course
www.sans.org/ondemand

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/rocky-mountain-2017/courses

SEC542:

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

Web applications play a vital role in every modern organization. But if your organization does not properly **test** and **secure** its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. **Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions.** Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

"Excellent materials, excellent presentation, and everything was spot-on. The instructor gave a really good overview of the essential topics." -Mark Jayson Alvarez, Asurion

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. **This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way to hammer home lessons learned.**

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

Bundle OnDemand
with this course
www.sans.org/ondemand

"Micah's knowledge gave me a better perspective on the development process, and helped peel back the onion on infrastructure and environments. This was a great course with a lot of good info!" -Ephraim P., U.S. Air Force

Micah Hoffman *SANS Certified Instructor*

Micah Hoffman has been working in the information technology field since 1998 supporting federal government and commercial customers in their efforts to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide excellent solutions to his customers. Micah holds the GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP. Micah is an active member in the NoVAHackers community, writes Recon-ng modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on the Appalachian Trail or the many park trails in Maryland. @WebBreacher

SEC560:

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

ALSO AVAILABLE VIA SIMULCAST

See page 17 for details.

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

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

"Kevin keeps the topic interesting and I am able to pick up key points by the way he keys in on the topic."
-Christian Campbell, nGuard, Inc.

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.

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.

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.**

Who Should Attend

- Security personnel whose jobs involve 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

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 for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, 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 also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. @kevinbfiscus

SANS

FOR508:

Advanced Digital Forensics, Incident Response, and Threat Hunting

Six-Day Program
Mon, June 12 - Sat, June 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

www.giac.org/gcfa

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools. The key is to catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization. For the incident responder, this process is known as "threat hunting."

"This is a fantastic course and Rob is a fantastic instructor with real-world application experience. FOR508 is a must for any investigator." -Eddie Sky, Forsythe Technology

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, this course addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy, 2nd Edition*. Rob is also co-author of the MANDIANT threat intelligence report *M-Trends: The Advanced Persistent Threat*. @robtlee & @sansforensics

FOR578:
Cyber Threat Intelligence

Five-Day Program
Mon, June 12 - Fri, June 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Scott Roberts

"Outstanding course material and instructor presentation! It truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."
-Thomas L., U.S. Air Force

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 (APTs)
- 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 (IOCs) 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.

"Fantastic class! I love the way the terminology was covered. I will be making index cards to ensure I have them memorized." -Nate DeWitt, eBay, Inc.

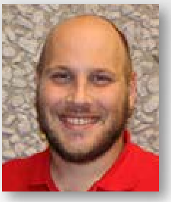
Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence 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-level 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!

Who Should Attend

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



Scott Roberts *SANS Instructor*

Scott Roberts is an incident responder, manager, and developer at GitHub, the world's code collaborative development platform. Scott has worked major investigations involving criminal fraud and abuse and nation-state espionage while with Symantec, Mandiant, and others. He is a sought-after speaker, having presented on threat intelligence and incident response for SANS, Silicon Valley, and various BSides. He is an author of O'Reilly's upcoming *Intelligence Driven Incident Response*. Scott is also a member of the SANS CTI Summit and NYU Poly CSAW Advisory Boards. @sroberts

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, June 12 - Fri, June 16
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. In addition, 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.

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.

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 their technical people are telling them

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

www.giac.org/gslc

www.sans.edu

www.sans.org/8140

▶❚❚
Bundle OnDemand
with this course
www.sans.org/ondemand

"This course is very comprehensive and provides excellent awareness of how web servers and interaction work. Worth your time!"
-Steve McGee,
Curaspan Health Group

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for InfoSec, public key infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he has bachelor's degrees in computer science and mathematics, and master's degrees in business administration and strategic studies, along with the GSLC, CISSP, CISM, and CISA certifications. @g_mark

ICS410: ICS/SCADA Security Essentials

Five-Day Program
Mon, June 12 - Fri, June 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Billy Rios

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

> "This course was a great introduction into the ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company." -Mike Poulos, Coca-Cola Enterprises

Given the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity.

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

Billy Rios *SANS Instructor*

An accomplished author and speaker, Billy is recognized as one of the world's most respected experts on emerging threats related to industrial control systems (ICS), critical infrastructure, and medical devices. He has discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publicly credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy was a Lead at Google, where he led the front-line response to externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company's response to several high-profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active-duty Marine Corps Officer. He holds an MBA and a Master of Science in Information Systems. He was a contributing author for several publications including *Hacking, the Next Generation* (O'Reilly), *Inside Cyber Warfare* (O'Reilly), and *The Virtual Battle Field* (IOS Press). @XSSniper

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/rocky-mountain-2017/courses

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: Welcome Threat Hunters, Phishermen, and Other Liars – *Rob Lee*

Over the past few years, a new term has continually popped up in the IT Security community: "threat hunting." While the term seems like it is new, it is in fact the reason why all of us joined IT security in the first place. The concept and root idea of threat hunting is nothing new. When I first started in IT Security back in the late 1990s, my job was to find threats in the network. This led to automated defenses such as Intrusion Detection Systems, monitoring egress points, logging technology, and monitoring the defensive perimeter hoping nothing would get in. Today, while the community is trying to identify intrusions, threat hunting has evolved to be something a bit more than the loose definition of "find evil" primarily due to the massive amount of incident response data currently collected about our attackers. This data has evolved into Cyber Threat Intelligence. This talk was put together to outline what exactly "threat hunting" means and will step you through exactly how it works.

Quality Not Quantity: Continuous Monitoring's Deadliest Events – *Eric Conrad*

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to the firm's SOC during the breach but missed...lost in the noise of millions. If you are bragging about how many events your SOC handles each day, you are doing it wrong. During this talk we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach. We will also provide an overview of DeepBlueCLI, a PowerShell framework for automatically detecting the deadliest events.

Anti-Ransomware: How to Turn the Tables – *G. Mark Hardy*

"OMG! We just got hit with ransomware!" What you don't usually hear next is, "LOL!" You can build defenses that prevent ransomware from paralyzing your organization – we'll show you how. Ransomware is a billion dollar industry, and it's getting even bigger. Lost productivity costs far more than the average ransom, so executives just say, "Pay the darn thing." But what if you could stop ransomware in its tracks? We'll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector, and venture predictions on how this industry will evolve and what to expect next.

So, You Wanna Be a Pentester? – *Adrien de Beaupre*

This presentation will discuss the things that you will actually need to become a penetration tester. Be prepared for a no-fluff honest discussion!

Collecting and Exploiting Your "Private" Internet Data Using OSINT

Micah Hoffman

Have you ever wondered how an attacker gets access to the data you, your family and friends post to the Internet? What could they do with it? Could they find your spouse and family members from your profile information? What tools and techniques do they leverage in their Open Source Intelligence (OSINT) research on potential victims? If you have wondered (and worried) about this, then you need to come to this talk. We will walk through how an attacker can leverage Burp Suite, Recon-ng and a variety of Internet resources to gather OSINT on potential targets. We will use search engines to locate target homes, learn about the psychology behind why people share what they do, and learn some effective methods of protecting your private Internet data.

Internet of Things (IoT) and Embedded Device Security Research – A Primer – *Billy Rios*

IoT and embedded devices are all around us, radically changing the world we live in. Have you ever wondered how these devices work? Are you interested in hacking these devices? Let's crack open an embedded device and learn how typical consumer devices are architected and built. We'll also cover some of the essential tools needed for device research and we'll discuss how these tools are used during a typical device review. As we cover various device weaknesses, we'll discuss some of the common pitfalls embedded researchers face and explore various ways to protect devices against specific device weaknesses.

CORE NETWARS EXPERIENCE

Test your cybersecurity knowledge and skills LIVE at

SANS Rocky Mountain 2017 with 2 free nights of NetWars!

THU, JUNE 15 – FRI, JUNE 16 6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS ROCKY MOUNTAIN 2017**. External participants are welcome to join for an entry fee of $1,520.

SANS NetWars is a dynamic cyber range that allows participants to build, practice, and measure their skills in a real-world environment using defensive, analytic, and offensive tactics. We designed NetWars to appeal to a wide range of participant skill sets by using a system with different levels.

All players start at Level 1, which measures foundational cybersecurity skills. More skilled players can rise rapidly through the ranks to a level suitable for their skill set – top players can make it to Level 4, and only the best of the best can reach level 5.

sans.org/rocky-mountain

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

Start your first course at Rocky Mountain 2017.

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

GI Bill

Tuition Reimbursement

Regional accreditation enables students to use corporate tuition reimbursement.

The SANS Technology Institute is also approved to accept and/or certify Veterans for education benefits.

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.

GIAC
CERTIFICATIONS

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

www.sans.edu | info@sans.edu

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.

GIAC CERTIFICATIONS

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.

Future Training Events

Pen Test Austin	Austin, TX	Mar 27 - Apr 1

SANS 2017	Orlando, FL	Apr 7-14
Baltimore Spring	Baltimore, MD	Apr 24-29

Security West	San Diego, CA	May 9-18
Northern Virginia – Reston	Reston, VA	May 21-26
Atlanta	Atlanta, GA	May 30 - June 4
Houston	Houston, TX	June 5-10
San Francisco Summer	San Francisco, CA	June 5-10
Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia	Columbia, MD	June 26 - July 1
Los Angeles - Long Beach	Long Beach, CA	July 10-15

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

Future Summit Events

Threat Hunting and IR	New Orleans, LA	Apr 18-25
Automotive Cybersecurity	Detroit, MI	May 1-8
Security Operations Center	Washington, DC	June 5-12
Digital Forensics	Austin, TX	June 22-29
ICS & Energy	Houston, TX	July 10-14
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2

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

Embassy Suites Denver Downtown Convention Center

1420 Stout Street | Denver, CO 80202
303-592-1000
sans.org/event/rocky-mountain-2017/location

The Embassy Suites Denver Downtown Convention Center hotel offers the perfect setting for business or pleasure. The hotel is a gateway to Denver's lively downtown scene. Boasting a contemporary convention venue, the hotel is within walking distance of the best attractions in the downtown area.

Special Hotel Rates Available

A special discounted rate of $205.00 on single/double occupancy will be honored based on space availability.

Limited 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 guest-room Internet, a cooked-to-order breakfast buffet, and daily manager's reception. Rates are only available through **Friday, May 19, 2017**.

Top 5 reasons to stay at the Embassy Suites Denver Downtown

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 Embassy Suites Denver Downtown 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 Embassy Suites Denver Downtown that you won't want to miss!

5 Everything is in one convenient location!

Registration Information

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

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.

SANS Simulcast

To register for a SANS Rocky Mountain 2017 Simulcast course, please visit www.sans.org/event/rocky-mountain-2017/attend-remotely

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**4-19-17**	**$400.00**	**5-10-17**	**$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 **May 24, 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