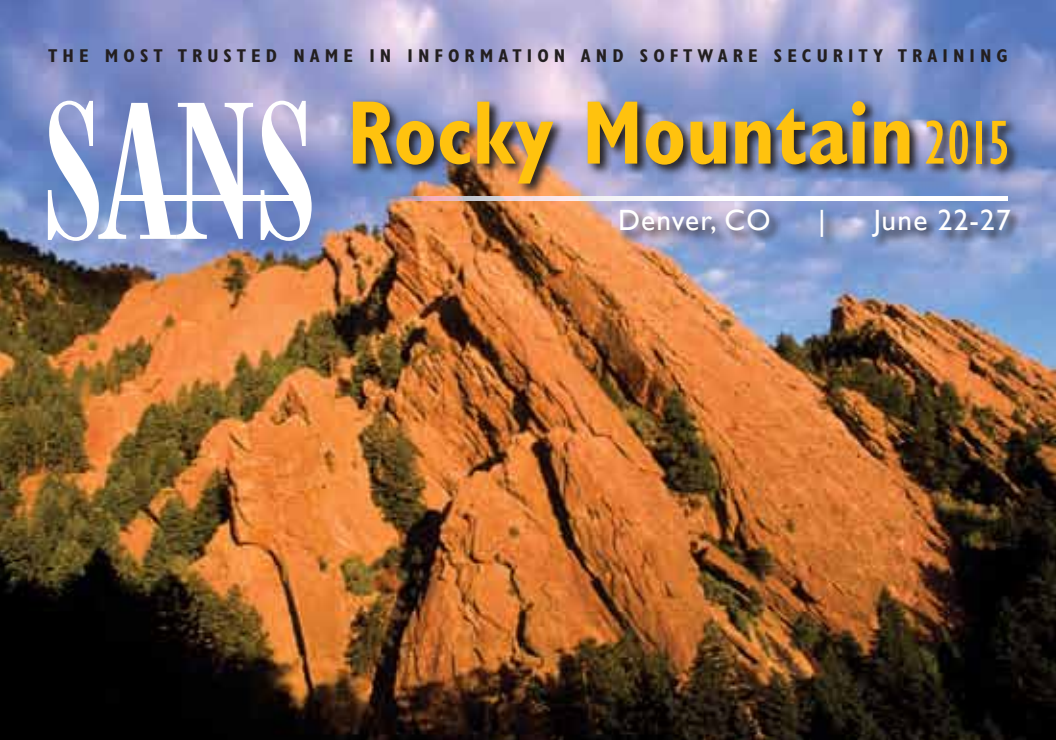
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Rocky Mountain 2015

Denver, CO | June 22-27



Choose from these popular courses:

SEC301: **Intro to Information Security NEW!**

SEC401: **Security Essentials Bootcamp Style**

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**

SEC560: **Network Penetration Testing and Ethical Hacking**

SEC503: **Intrusion Detection In-Depth**

MGT414: **SANS Training Program for CISSP Certification®**

SEC575: **Mobile Device Security and Ethical Hacking**

ICS410: **ICS/SCADA Security Essentials**

"SANS has exceeded my expectations and successfully refocused my view of threats and risks."

-Charles Allen, EMSolutions, Inc.

GIAC Approved Training

Register at
sans.org/event/rocky-mountain-2015

Save $400
Register & pay early!
See page 13 for more details.

SANS invites you to attend **Rocky Mountain 2015** to get the intensive immersion cybersecurity training you need to defend your systems and networks against the most nefarious cyber threats. The training event will be held in the mile-high city of Denver from June 22-27.

Enterprises are scrambling to find trained and certified professionals with the knowledge and hands-on skills to defend their companies against targeted and customized cyber attacks. SANS training teaches you the practical steps and techniques you need to take on those challenges as soon as you get back to your office.

Rocky Mountain 2015 features a lineup of eight courses, including IT security, penetration testing, CISSP certification, mobile devices, incident handling, and ICS/SCADA. The courses are taught by world-class practitioners focused on scaling up your cybersecurity knowledge thoroughly and rapidly. The SANS team includes such well-known industry experts as Dr. Eric Cole, Mike Poor, Dave Shackleford, Eric Conrad, Bryce Galbraith, Christopher Crowley, Keith Palmgren, and Eric Cornelius. This brochure provides detailed information about the courses, faculty bios, certifications, hotel registration, and evening talks for Rocky Mountain 2015. The event features a number of extra bonus sessions that are free with your paid tuition and a great enhancement to your classroom training.

All of the courses offered at Rocky Mountain 2015 are GIAC certified. More and more students are telling us that GIAC certifications are vital to their careers. To find out how to sign up at a reduced rate, go to the GIAC page in this brochure or to the GIAC website at **giac.org**. Rocky Mountain 2015 also offers four courses that are in alignment with the DoD Directive 8570 (SEC401, SEC503, SEC504, and MGT414).

Advance your career by enrolling in a master's degree or graduate certificate program from the SANS Technology Institute, which is regionally accredited and eligible for tuition reimbursement plans. Choose from a master's in Information Security Engineering or a Graduate Certificate in Penetration Testing or Incident Response. Apply today! For more information, see the SANS Technology Institute page or go to **sans.edu**.

Rocky Mountain 2015 will be held at the Downtown Convention Center Embassy Suites, within walking distance of Denver's lively downtown scene. The hotel offers a picturesque panorama of the mountains surrounding the city. A special discounted rate of $199.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through June 4. See our location page for complete information.

Save $400 on any course by entering the discount code "**EarlyBird15**" during registration and completing payment by April 29, 2015.

Register today for SANS Rocky Mountain 2015! We look forward to seeing you in Denver!

Here's what SANS alumni have said about the value of SANS training:

"This knowledge is indispensable, utterly necessary, and relevant to every industry."
-Paul Ryan, GDIT

"This event gave me some food for thought and made me rethink my approach on security."
-David H. Neilson, Western Family Foods

"The course provided good examples and real-world data to support the statements made by the instructor."
-Bill Whitledge, VDR

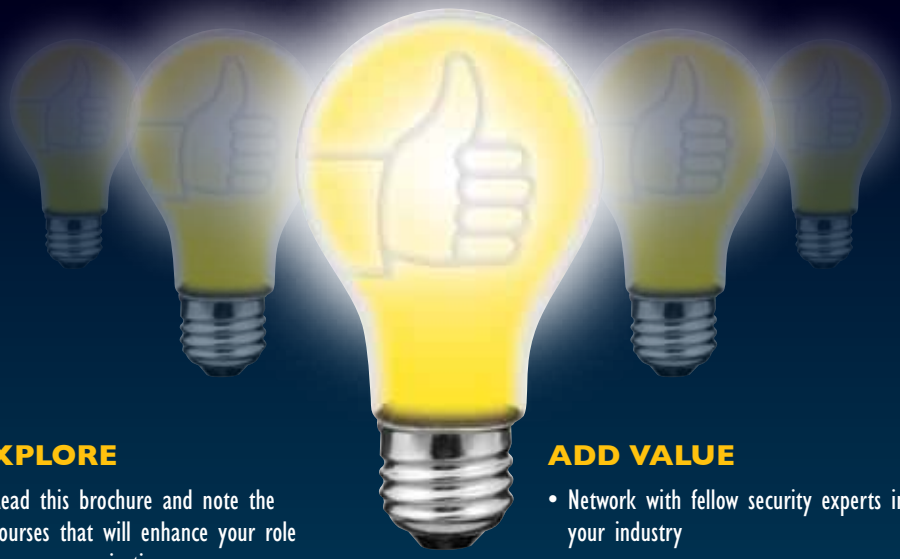
"Excellent talk really added value to the training I've received this week."
-R. Pilkington, CERT-UK

Courses-at-a-Glance

		MON 6/22	TUE 6/23	WED 6/24	THU 6/25	FRI 6/26	SAT 6/27
SEC301	Intro to Information Security NEW!	Page 2					
SEC401	Security Essentials Bootcamp Style	Page 3					
SEC503	Intrusion Detection In-Depth	Page 4					
SEC504	Hacker Tools, Techniques, Exploits & Incident Handling	Page 5					
SEC560	Network Penetration Testing and Ethical Hacking	Page 6					
SEC575	Mobile Device Security and Ethical Hacking	Page 7					
MGT414	SANS Training Program for CISSP Certification®	Page 8					
ICS410	ICS/SCADA Security Essentials	Page 9					

@SANSInstitute *Join the conversation:* #SANSRockyMtn

The Value of SANS Training & YOU



EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

SECURITY 301

Intro to Information Security

NEW

SANS

Five-Day Program
Mon, June 22 - Fri, June 26
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Keith Palmgren
- GIAC Cert: GISF
- OnDemand Bundle

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management.

Who Should Attend

- Persons new to information technology who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and Information Security Officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss Internet Protocol, routing, Domain Name Service, and network devices. We cover the basics of cryptography, security management, and wireless technology, then we look at policy as a tool to effect change in your organization. On the final day of the course, we put it all together with an implementation of defense in-depth.

If you're a newcomer to the field of information security, this course will start you off with a solid foundation. SEC301 will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.

"Really interesting course – I feel as if I'm getting a great overview of security, and I now know the areas where I need more training to best get my job done."
Rachel Shaw, Qualcomm Incorporated

"I love this SANS course. SEC301 was very helpful for someone new to the field."
Amanda Massey, Capital Bank

GISF
giac.org

▶II
BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Keith Palmgren *SANS Certified 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 & 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 a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, June 22 - Sat, June 27
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Dr. Eric Cole

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

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

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"I really enjoyed the topics. In addition, it brought a lot of stuff together that is related directly to my job and the things I have to deal with."
-Bryan Chou, Murphy USA

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drericcole

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, June 22 - Sat, June 27
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Mike Poor

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

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

Who Should Attend

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

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

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

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

"Mike is outstanding! Many claim to have the background and knowledge that he does, but it's nice to learn from a real pro!"
-Jeremy Glass, Molina Healthcare

"Awesome course! Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

"The amount of knowledge and experience that Mike has, I don't think you could get that from any other organization other than SANS."
-Hayley Roberts, MOD

Mike Poor *SANS Senior Instructor*

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

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, June 22 - Sat, June 27
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Bryce Galbraith

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

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

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This training is comprehensive, thought provoking, and directly relevant to today's security needs. What I learned here today, I can directly apply tomorrow at my job."
-Shannon Steinfadt

"Purely amazing class! Tons of great information, and easy to follow examples."
-Adam Candi, Trustware Holdings

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he 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, he holds several security certifications and speaks at conferences around the world. @brycegalbraith

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, June 22 - Sat, June 27
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Dave Shackleford

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

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

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

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

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

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

giac.org

sans.edu

sans.org/
cyber-guardian

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"As someone new to information security this course helped me understand what is possible and what mindset is needed to work against this."
-Travis Knox, FirstBank

"This training is extremely important, given the nature of DOD networks. The best answers to compromising a system are likely going to be the hardest to implement."
-David Poulin,
7th Cyber Protection Brigade

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

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Mon, June 22 - Sat, June 27
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Christopher Crowley

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

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This course is hard but very rewarding. I really appreciated the insight and it gives me the building blocks to continue in this field."
-Tony Maurer, DIBP

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient e-mail access as well by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **The high probability of device loss or theft, and more**

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

This course is designed to help organizations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course will help you build the critical skills to support your organization's secure deployment and use of mobile phones and tablets. You will learn how to capture and evaluate mobile device network activity, disassemble and analyze mobile code, recognize weaknesses in common mobile applications, and conduct full-scale mobile penetration tests.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley 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. Mr. Crowley is the course author for SANS Management 535 - 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, 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

MANAGEMENT 414

SANS Training Program for CISSP Certification®

Content Updated for New Exam! Effective April 15th

SANS

Six-Day Program
Mon, June 22 - Sat, June 27
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Eric Conrad

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

SANS offers the first course updated for the 2015 version of the CISSP® exam. Eric Conrad and Seth Misenar, authors of the bestselling Syngress CISSP® Study Guide, have fully updated the course to address the 2015 version of the CISSP® exam.

MGT414: SANS Training Program for CISSP® Certification is an accelerated review course designed to prepare you to pass the exam. The course takes into account the 2015 updates to the CISSP® exam and prepares students to navigate all types of questions included on the new version of the exam.

Who Should Attend

- Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)².
- Managers who want to understand the critical areas of network security.
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 8 domains.
- Security professionals and managers looking for practical ways to apply the 8 domains of knowledge to their current activities.

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

After completion of this course, students will have a strong working knowledge of the 8 domains of knowledge and be better placed to pass the exam.

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

"Eric did an amazing job teaching the class. It was a lot of material, but he did a good job of keeping the class going. I'll be back for future classes."
-Axel Persaud, University of Maryland

You Will Be Able To:

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

giac.org


sans.org/8570

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

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

Eric Conrad *SANS Principal 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 health care. 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 as a Master of Science 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 www.ericconrad.com. @eric_conrad

INDUSTRIAL CONTROL SYSTEMS 410

ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, June 22 - Fri, June 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Eric Cornelius
- GIAC Cert: GICSP
- OnDemand Bundle

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.

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

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.

When students complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This training has definitely empowered me some more with knowledge above standards. I believe that if I apply the leaning I received here, I will be able to perform as a network engineer & CS-IT with more expertise."
-Robin U. Familara, CGI

"Very satisfied with ICS410, and the instructor was very knowledgeable and great at balancing group backgrounds (IT vs. SCADA)."
-Chad Slater,
The Dow Chemical Company

Eric Cornelius *SANS Instructor*

Eric Cornelius is currently a Technical Director at Cylance, Inc. and has recently served as the Chief Technical Analyst for DHS CSSP. As an active researcher in the field of cybersecurity since 2002, Mr. Cornelius supported many "boots-on-the-ground" engagements involving penetration testing, forensics, and malware analysis. Through these engagements, Mr. Cornelius aided multiple government, military, and private-sector organizations in protecting their networks and industrial control systems.

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: Who's Watching the Watchers? *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation and aggregation... but do we know if we have it right? Will we detect the NextGen™ attackers. In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

Jailbreak/Root Workshop for Mobile Devices *Chris Crowley*

This talk is primarily a hands-on workshop with a brief discussion of tools for jailbreak of vulnerable iOS and Android platforms. Bring an older iOS device (an iPhone 3GS from ebay will work great) or a Nexus 7 tablet (or Nexus 4 phone) to root or jailbreak. This session is intended to allocate time to jailbreak and root devices to help SEC575 attendees understand the methods available for unrestricting mobile devices. The unrestricted device is useful for application assessments and pen testing.

WARNING: The techniques discussed could render the devices completely inoperable. Bring a device that can become unusable without you becoming upset.

Why Our Defenses Are Failing Us. One Click Is All It Takes. *Bryce Galbraith*

Organizations are spending unprecedented amounts of money in an attempt to defend their assets—yet all too often, one click is all it takes for everything to come toppling down around them. Every day we read in the news about national secrets, intellectual property, financial records, and personal details being exfiltrated from the largest organizations on earth. How is this being done? How are adversaries bypassing our defenses (e.g. strong passwords, non-privileged accounts, anti-virus, firewalls/proxies, IDS/IPS, logging, etc.)? And most importantly, what can we do about it? A keen understanding of the true risks we face in today's threatscape is paramount to keeping your ones and zeros where they belong.

The 13 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified thirteen absolute truths of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves, and even for their children.

FUTURE SANS TRAINING EVENTS

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

SANS Security West 2015
San Diego, CA | May 3-12 | #SecurityWest

SANS Pen Test Austin 2015
Austin, TX | May 18-23 | #PenTestAustin

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS Capital City 2015
Washington, DC | July 6-11 | #SANSCapitalCity

SANS San Jose 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS Minneapolis 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS Boston 2015
Boston, MA | August 3-8 | #SANSBoston

SANS San Antonio 2015
San Antonio, TX | August 17-22 | #SANSSATX

SANS Virginia Beach 2015
Virginia Beach, VA | Aug 24 - Sept 4 | #SANSVaBeach

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

Private Training sans.org/private-training
Live Onsite Training at Your Office Location. Both in Person and Online Options Available

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

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

ONLINE TRAINING

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

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

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

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

SANS ROCKY MOUNTAIN 2015

Hotel Information

Training Campus

Embassy Suites Denver Downtown Convention Center

1420 Stout Street | Denver, CO 80202

sans.org/event/rocky-mountain-2015/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 $199.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through June 4, 2015.

Top 5 reasons to stay at the Embassy Suites Denver Downtown Convention Center

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Embassy Suites Denver Downtown Convention Center, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Embassy Suites Denver Downtown Convention Center that you won't want to miss!
5. Everything is in one convenient location!

SANS ROCKY MOUNTAIN 2015

Registration Information

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

Register online at sans.org/event/rocky-mountain-2015/courses

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

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**4/29/15**	**$400.00**	**5/27/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

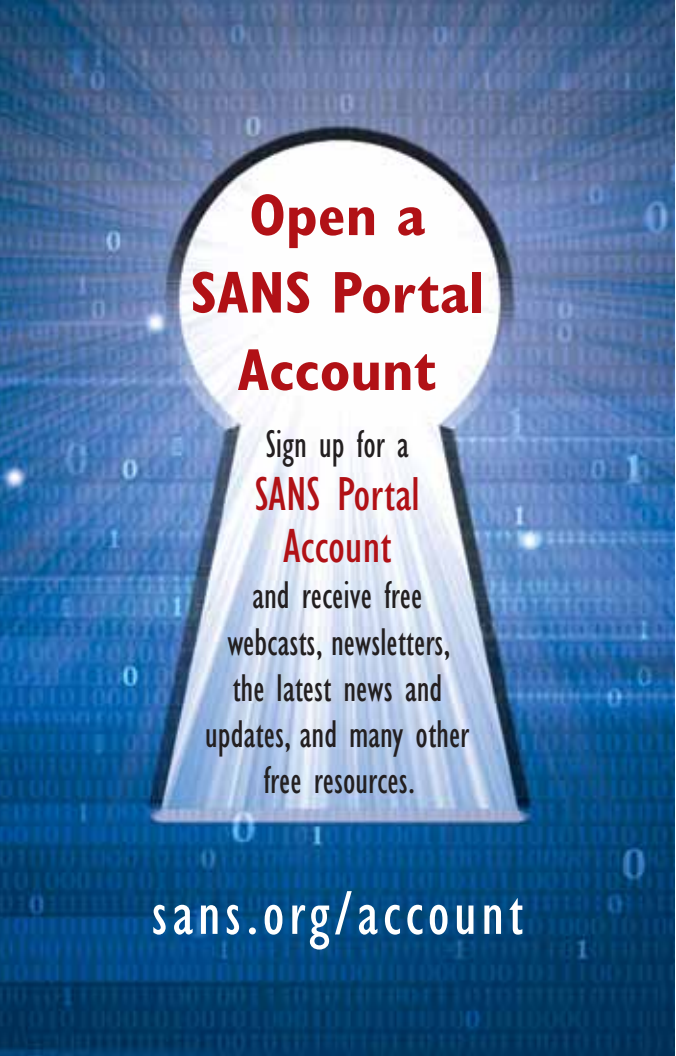
To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by June 3, 2015 – processing fees may apply.

SANS Voucher Credit Program

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


Open a
SANS Portal
Account
Sign up for a
SANS Portal
Account
and receive free
webcasts, newsletters,
the latest news and
updates, and many other
free resources.
sans.org/account