INFORMATION SECURITY TRAINING

Protect Your Business | Advance Your Career

Eight hands-on, immersion-style courses taught by real-world practitioners

See inside for courses offered in:
- Cyber Defense
- Penetration Testing
- Ethical Hacking
- Security Management
- CISSP® Preparation
- Digital Forensics
- ICS/SCADA Security

“When you want to be the best, you train with the best.”
- Daniel Bergeron, Global Excel Management Inc.

Boston Spring 2018
March 25-30

SAVE $400
Register and pay by Jan 31st
Use code EarlyBird18

www.sans.org/boston-spring
Evening Bonus Sessions
Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11.

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

Adversary Simulations: Taking Attack Models and Penetration Testing to the Next Level
Jorge Orchilles

Using the Attack and Defense Matrix Scorecard
Mick Douglas

Save $400 when you register and pay by January 31st using code EarlyBird18
Securing Approval and Budget for Training

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

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

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

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

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.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

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

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

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. Our course will show you how to prevent your organization’s security problems from being headline news in the Wall Street Journal!

Prevention is ideal but detection is a must.

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

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

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

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. Our course will show you how to prevent your organization’s security problems from being headline news in the Wall Street Journal!

Prevention is ideal but detection is a must.

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

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

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

Who Should Attend

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

“Thank you SANS for a deeply challenging and rewarding week of learning.”

- Chris Drews, 3M

Tim Garcia  SANS Certified Instructor

Tim Garcia is a seasoned security professional who loves the challenging and continuously changing landscape of defense. Tim currently works as an information security engineer for a Fortune 100 financial company, where he helps project teams ensure the security of IT operations and compliance with policies and regulations. He also leads the team that is tasked with firewall review, SIEM management and privileged access monitoring and policy compliance. Tim has worked as a systems engineer and database administrator and has expertise in systems engineering, project management and information security principles and procedures/compliance. Tim previously worked for Intel and served in the U.S. Navy. At SANS, Tim also works with the OnDemand team as a subject-matter expert, serves as a mentor for the Vet Success program, and provides consulting and content review for the Securing The Human project. Tim is a contributor to the Arizona Cyber Warfare Range and works with the local security community giving monthly talks on information security tools and techniques. Tim holds the CISSP, GSEC, GCISO, GCFI, GMON, GW2MN, GCCC, GCED, and MSA-IMA certifications. He has extensive knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, Cobit, COSO, and ISO 17799. @tbg911

Register at www.sans.org/boston-spring | 301-654-SANS (7267)

www.sans.edu

www.giac.org/gsec

www.sans.org/8140

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

As someone who works in information security but has never had to do a full incident report, SEC504 taught me all the proper processes and steps.

- Todd Choryan, Motorola Solutions

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

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

Mick Douglas  SANS Certified Instructor

Even when his job title has indicated otherwise, Mick Douglas has been doing information security work for over 10 years. He received a bachelor’s degree in communications from Ohio State University. He is the managing partner for InfoSec Innovations. He is always excited to have the opportunity to share with others so they do not have to learn the hard way! By studying with Mick, security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he’s not “geeking out” you’ll likely find Mick indulging in one of his numerous hobbies: photography, scuba diving, or hanging around in the great outdoors.

@BetterSafetyNet
Web applications play a vital role in every modern organization. However, if your organization doesn’t 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.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

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, and 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.

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll 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, not just show off hacking skills. This course will help students demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having 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 that hammers home lessons learned.
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 take on this challenge.

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

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

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

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

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

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.

“I like that the labs in SEC560 provided clear, step-by-step guidance. The instructor’s level of knowledge and ability to relay information is fantastic.”
- Bryan Barnhart, Infiltration Labs

Jorge Orchilles
SANS Instructor

Jorge Orchilles, author of Microsoft Windows 7 Administrator’s Reference, holds a bachelor of business administration in management information systems from Florida International University. He leads the advanced penetration testing and vulnerability assessment quality control teams at a large financial institution and serves on the board of the South Florida Chapter of the Information Systems Security Association. Jorge holds various certifications from ISC2, ISACA, SANS GIAC, EC-Council, Cisco, Microsoft, and CompTIA, including GXPN, CISSP, CISM, GPEN, GCIH, CIEH, CICP, CCDA, SSSE, CompTIA Security+ (2008), Microsoft Certified Professional (70-228, 70-282, 70-284) and Microsoft Certified Technology Specialist (70-620). Jorge speaks Spanish and Portuguese in addition to English.

@jorgeorchilles
Advanced Digital Forensics, Incident Response, and Threat Hunting

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

- 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

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 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.

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, FOR508 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!

I appreciate that the instructor is able to teach to many levels and breaks everything down to make it easy to understand while still maintaining/providing useful/high-level information.”

- Alicia Murphy, Booz Allen Hamilton

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.”

Mike Pilkington SANS Certified Instructor

After spending much of his career as an analyst and incident responder for Halliburton, Mike recently joined the team at Shell. In his current role as a senior incident analyst at Shell, Mike regularly deals with malware and intrusion cases. His work ranges from evaluating and implementing both commercial and open-source forensic tools to consulting with internal groups to resolve intrusions. He has accumulated a broad range of technical expertise, having spent significant time performing software quality assurance, Windows systems administration, LAN and WAN network administration, firewall and IDS/IPS security administration, computer forensic analysis, and incident response. Mike holds a bachelor’s degree in mechanical engineering from the University of Texas, as well as numerous IT security certifications, including the CISSP, EnCE, GCFE, GCFA, and GREM.

SANS Certified Instructor

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.”

Mike Pilkington SANS Certified Instructor

After spending much of his career as an analyst and incident responder for Halliburton, Mike recently joined the team at Shell. In his current role as a senior incident analyst at Shell, Mike regularly deals with malware and intrusion cases. His work ranges from evaluating and implementing both commercial and open-source forensic tools to consulting with internal groups to resolve intrusions. He has accumulated a broad range of technical expertise, having spent significant time performing software quality assurance, Windows systems administration, LAN and WAN network administration, firewall and IDS/IPS security administration, computer forensic analysis, and incident response. Mike holds a bachelor’s degree in mechanical engineering from the University of Texas, as well as numerous IT security certifications, including the CISSP, EnCE, GCFE, GCFA, and GREM.

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 FOR500 and SEC504 graduates

“...
Six-Day Program  
Sun, Mar 25 - Fri, Mar 30  
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: Seth Misenar

Who Should Attend

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

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

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

Obtaining Your CISSP® Certification Consists of:

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

“I have taken several CISSP® prep courses in the last several years and this by far is the best. Finally I feel that I have the confidence to take the test.”  
-Jerry Carse, Sarum, LLC

“This training was a comprehensive overview of all topics covered on the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless.”  
-Ron Pinnock, Navy Exchange Service Command

“I think the course material and the instructor are very relevant for the task of getting a CISSP®. The overall academic exercise is solid.”  
-Aaron Lewter, Availity

Seth Misenar  SANS Senior Instructor

Seth Misenar is the founder and lead consultant for Context Security, a Jackson, Mississippi-based company that provides information security thought leadership, independent research, and security training. Seth’s background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has served as both a physical and network security consultant for Fortune 100 companies and the Health Insurance Portability and Accountability Act, as well as an information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor’s degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include the CISSP, GPEC, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/boston-spring-2018/courses

www.giac.org/gisp  
SANS Training Program for CISSP® Certification  
Information Security Professional  
www.sans.org/8140  
www.sans.org/ondemand
MGT512

SANS Security Leadership Essentials for Managers
with Knowledge Compression™

Five-Day Program
Sun, Mar 25 - Thu, Mar 29
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: Ted Demopoulos

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it’s like drinking from a fire hose. The diligent manager will gain the vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

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.

“MG512 has excellent coverage of what matters for the leadership/management portion. Also, no B.S. – very concrete.”
- Hervé Loterie, Proximus

“Excellent material geared directly to management principles that can be applied in any organization.”
- Tom Kleis, DoN civilian at CSCS

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!

Ted Demopoulos  SANS Principal Instructor
Ted Demopoulos’ first significant exposure to computers was in 1977 when he had unlimited access to his high school’s PDP-11 and hacked at it incessantly. He consequently almost flunked out, but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a “textbook failure” of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events and is quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is also a food and wine geek, goes flyfishing, and enjoys playing with his children. #TedDemop
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 ICS410 course helped open my eyes to Industrial Control Systems and the complexities of securing them. It helped me clearly understand how to think about and implement cybersecurity in the industrial landscape.”

-Ken Coyner, AT&T

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.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, 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. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals 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.

Paul (Monta) Elkins  SANS Instructor

Monta Elkins is currently “Hacker-in-Chief” for FoxGuard Solutions, an ICS patch provider. A security researcher and consultant, he was formerly Security Architect for Rackspace, and served as the first ISO for Radford University. He has been a speaker at DEFCON, the Department of Homeland Security’s Industrial Control Systems Joint Working Group, EnergySec’s Security Summit, VASCAN, GE Digital Energy’s Annual Software Summit, the Educase Security Professionals Conference, Toshiba’s Industrial Control Systems Conference, NERC’s GridSecCon, ICS CyberSecurity by Security Week, UTC Telecom, and other security conferences. Monta is the author and instructor of the “Defense against the Dark Arts” hands-on, hacker tools and techniques classes. He is also a guest lecturer for Virginia Tech University and teaches rapid prototyping and Arduino classes with Let’s Code Blacksburg. @montaelkins

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

The course is designed for those with a basic understanding of control systems and IT/OT support who are interested in developing a foundational level of focus as system reliability throughout the system lifecycle.

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 ICS410 course helped open my eyes to Industrial Control Systems and the complexities of securing them. It helped me clearly understand how to think about and implement cybersecurity in the industrial landscape.”

-Ken Coyner, AT&T

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.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, 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. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals 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.

Paul (Monta) Elkins  SANS Instructor

Monta Elkins is currently “Hacker-in-Chief” for FoxGuard Solutions, an ICS patch provider. A security researcher and consultant, he was formerly Security Architect for Rackspace, and served as the first ISO for Radford University. He has been a speaker at DEFCON, the Department of Homeland Security’s Industrial Control Systems Joint Working Group, EnergySec’s Security Summit, VASCAN, GE Digital Energy’s Annual Software Summit, the Educase Security Professionals Conference, Toshiba’s Industrial Control Systems Conference, NERC’s GridSecCon, ICS CyberSecurity by Security Week, UTC Telecom, and other security conferences. Monta is the author and instructor of the “Defense against the Dark Arts” hands-on, hacker tools and techniques classes. He is also a guest lecturer for Virginia Tech University and teaches rapid prototyping and Arduino classes with Let’s Code Blacksburg. @montaelkins
Enhance Your Training Experience

Add an OnDemand Bundle OR GIAC Certification Attempt
to your course within seven days of this event to get bundle 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

OnDemand Bundle price – $729

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

-ROBERT JONES, TEAM JONES, INC.

Get Certified with GIAC Certifications

• Distinguish yourself as an information security leader
• 30+ GIAC cybersecurity certifications available
• Two practice exams included
• Four months of access to complete the attempt

GIAC bundle price – $729

“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.
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 all of us joined IT Security in the first place: to “find evil.” While I was at Mandiant and in the US Air Force, “finding evil” was our tagline while we were on engagements.

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. These data has evolved into Cyber Threat Intelligence (CTI).

It is hard to simply “go find evil,” but if armed with a bit of CTI in the mix – or essentially what you might be looking for, or what your adversaries are likely interested – can make your hunt more targeted. These indicators are used to great effect when employed properly and proactively against a threat group. Threat hunting has improved the accuracy of threat detection because now we can focus our search on the adversaries exploiting our networks – humans hunting humans. Even though we may now know where to look, new tools are still being introduced to help make hunting more practical across an enterprise.

This talk was put together to outline what exactly “threat hunting” means and will step you through exactly how it works.

**Adversary Simulations:**

**Taking Attack Models and Penetration Testing to the Next Level**

Jorge Orchilles

It is extremely rare that a single vulnerability causes a critical, direct risk to your entire environment. In reality, it is what the attacker does with the access gained that matters most. In this talk we will talk about maturing our attack models to gain enough intelligence to simulate the tactics, techniques, and procedures of the adversary against our entire environment. Attackers do not limit themselves to one application, instead they look at your organization holistically to formulate an attack that achieves their objectives. We will discuss an adversary simulation framework and share a case study of it in action.

**Using the Attack and Defense Matrix Scorecard**

Mick Douglas

Did you ever want to know how an attack may impact your system prior to running it? Did you ever want to know if your defenses are working as expected? Will the latest zero-day exploit go straight through your defense? Will the hot new exploit get you DA on your pen test? Come to this talk and find out!

By leveraging the MITRE ATT&CK Framework, we’ve developed a holistic view of how the layers of your security controls work – or don’t. Learn where you should be focusing your efforts. Find out what your biggest weaknesses are! Take your defensive or offensive game to the next level with this completely free and open tool.
### Future Training Events

#### Security East

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Winter</td>
<td>Reston, VA</td>
<td>Jan 15-20</td>
</tr>
<tr>
<td>Las Vegas</td>
<td>Las Vegas, NV</td>
<td>Jan 28 - Feb 2</td>
</tr>
<tr>
<td>Miami</td>
<td>Miami, FL</td>
<td>Jan 29 - Feb 3</td>
</tr>
<tr>
<td>Scottsdale</td>
<td>Scottsdale, AZ</td>
<td>Feb 5-10</td>
</tr>
<tr>
<td>Southern California</td>
<td>Anaheim, CA</td>
<td>Feb 12-17</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas, TX</td>
<td>Feb 19-24</td>
</tr>
<tr>
<td>New York City Winter</td>
<td>New York, NY</td>
<td>Feb 26 - Mar 3</td>
</tr>
<tr>
<td>San Francisco Spring</td>
<td>San Francisco, CA</td>
<td>Mar 12-17</td>
</tr>
<tr>
<td>Northern VA Spring – Tysons</td>
<td>McLean, VA</td>
<td>Mar 17-24</td>
</tr>
<tr>
<td>Pen Test Austin</td>
<td>Austin, TX</td>
<td>Mar 19-24</td>
</tr>
<tr>
<td>Boston Spring</td>
<td>Boston, MA</td>
<td>Mar 25-30</td>
</tr>
</tbody>
</table>

#### SANS 2018

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baltimore Spring</td>
<td>Baltimore, MD</td>
<td>Apr 21-28</td>
</tr>
<tr>
<td>Seattle Spring</td>
<td>Seattle, WA</td>
<td>Apr 23-28</td>
</tr>
</tbody>
</table>

#### Security West

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Reston Spring</td>
<td>Reston, VA</td>
<td>May 20-25</td>
</tr>
<tr>
<td>Atlanta</td>
<td>Atlanta, GA</td>
<td>May 29 - June 3</td>
</tr>
<tr>
<td>Rocky Mountain</td>
<td>Denver, CO</td>
<td>June 4-9</td>
</tr>
<tr>
<td>Crystal City</td>
<td>Arlington, VA</td>
<td>June 18-23</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>June 25-30</td>
</tr>
<tr>
<td>Vancouver</td>
<td>Vancouver, BC</td>
<td>June 25-30</td>
</tr>
</tbody>
</table>

#### Future Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threat Intelligence</td>
<td>Bethesda, MD</td>
<td>Jan 29 - Feb 5</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>San Diego, CA</td>
<td>Feb 19-26</td>
</tr>
<tr>
<td>ICS Security</td>
<td>Orlando, FL</td>
<td>Mar 19-26</td>
</tr>
<tr>
<td>Blue Team</td>
<td>Louisville, KY</td>
<td>Apr 23-30</td>
</tr>
<tr>
<td>Automotive Cybersecurity</td>
<td>Chicago, IL</td>
<td>May 1-8</td>
</tr>
<tr>
<td>DFIR</td>
<td>Austin, TX</td>
<td>June 7-14</td>
</tr>
</tbody>
</table>

#### Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.
Register online at www.sans.org/boston-spring
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.

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 February 28, 2018. 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.

Special Hotel Rates Available
A special discounted rate of $219.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed internet in your room and are only available through 5pm EST on March 2, 2018.

Top 5 reasons to stay at the Omni Parker House
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 Omni Parker House, 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 Omni Parker House that you won’t want to miss!
5. Everything is in one convenient location!

This grand luxury hotel has been symbolic of Boston’s rich history and culture since 1855. Old World charm and elegance are accompanied by all of the modern conveniences of a world-class establishment. Nestled in the heart of downtown Boston, Omni Parker House is located along the Freedom Trail and at the foot of Beacon Hill, Boston Common, Quincy Market and Faneuil Hall Marketplace. Omni Parker House is just 2.3 miles from Logan International Airport (10 minutes).

Omni Parker House
60 School Street
Boston, MA 02108
617-227-8600
www.sans.org/event/boston-spring-2018/location

Hotel Information

Register Information
Register online at www.sans.org/boston-spring
We recommend you register early to ensure you get your first choice of courses.
Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Pay Early and Save*
Pay & enter code by 1-31-18 $400.00
Pay & enter code by 2-21-18 $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 February 28, 2018. 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.
Newsletters

NewsBites
Twice-weekly, high-level executive summaries 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.

Webcasts

Ask the Experts 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 how a vendor’s commercial tool can be used to solve or mitigate that problem.

Other Free Resources (No portal account is necessary)

- 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)

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by December 27th. www.sans.org/dallas

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address. NALT-BRO-Dallas-2018