SANS

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

SALT LAKE CITY 2017

August 14-19

Protect Your Business and Advance Your Career

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

CYBER DEFENSE
PENETRATION TESTING
ETHICAL HACKING
DIGITAL FORENSICS
MANAGEMENT
ICS/SCADA SECURITY
CISSP® TRAINING

GIAC CERTIFICATIONS

"Hands-on, practical training requiring full attention and engagement in the learning sessions and labs. Just great!"
-Brent Pokornowski, ALLETE

SAVE $400

Register and pay by June 21st – Use code **EarlyBird17**

www.sans.org/salt-lake-city

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Salt Lake City 2017 lineup of instructors includes:

Ovie Carroll
Principal Instructor
@ovie

Chris Christianson
Certified Instructor
@cchristianson

Matt Edmondson
Instructor
@matt0177

Bryce Galbraith
Principal Instructor
@brycegalbraith

G. Mark Hardy
Principal Instructor
@g_mark

David R. Miller
Certified Instructor
@DRM_CyberDude

Justin Searle
Senior Instructor
@meeas

Evening Bonus Sessions

Take advantage of these extra evening presentations, and add more value to your training. Learn more on page 9.

KEYNOTE: ***Current and Future Trends in Digital Investigative Analysis***
Ovie Carroll

State of the Dark Web
Matt Edmondson

Control Things Platform
Justin Searle

Save $400 when you register and pay by June 21st using code EarlyBird17

Courses at a Glance

	MON 8-14	TUE 8-15	WED 8-16	THU 8-17	FRI 8-18	SAT 8-19
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC560 Network Penetration Testing and Ethical Hacking	Page 4					
FOR500 Windows Forensic Analysis (FORMERLY FOR408)	Page 5					
MGT414 SANS Training Program for CISSP® Certification	Page 6					
MGT514 IT Security Strategic Planning, Policy, and Leadership	Page 7					
ICS410 ICS/SCADA Security Essentials	Page 8					

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

Packaging matters

Write a formal request

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

Clearly state the benefits

Be specific

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

Set the context

Establish longer-term expectations

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

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, Aug 14 - Sat, Aug 19
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Chris Christianson

Who Should Attend

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

"This training answers the 'why' of my work practices, and asks the 'why not' for the practices my company doesn't follow."
-Thomas Petro, Southern California Edison

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

STOP and ask yourself the following questions:

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

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

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

Prevention Is Ideal but Detection Is a Must

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

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

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

SANS Technology Institute
www.sans.edu


www.sans.org/8140

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

Chris Christianson *SANS Certified Instructor*

Chris Christianson is an Information security consultant based in Northern California with 20 years of experience and many technical certifications including the CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, GWAPT, GISF, and GCED. He holds a Bachelor of Science degree in management information systems and was the assistant vice president in the information technology department at one of the nation's largest credit unions. Chris has also been an expert speaker at conferences and is a contributor to numerous industry publications. **@cchristianson**

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Aug 14 - Sat, Aug 19
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Matt Edmondson

Who Should Attend

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

"The course is brilliant. Very well run and easy to understand. If help was needed it came quick."
-Chris Clark, Inmarsat

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.**

"SEC504 is a good foundation for security incidents. It's a must-have for security incident handlers/managers."-Wu Peihui, Citibank

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. Additionally, 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.

"SEC504 helped me put many pieces of the puzzle together."
-Ian Trimble, Blue Cross Blue Shield

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian


www.sans.org/8140


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

Matt Edmondson *SANS Instructor*

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

SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester

www.giac.org/gpen

Six-Day Program
Mon, Aug 14 - Sat, Aug 19
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Bryce Galbraith

Who Should Attend

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

"It introduces the whole process of penetration testing from the start of engagement to the end."

-Barry Tsang, Deloitte

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

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

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with 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 extremely 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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally best-selling 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 he 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 curricula around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith

FOR500 (Formerly FOR408)

Windows Forensic Analysis

GCFE Certification
Forensic Examiner

www.giac.org/gcfe

Six-Day Program
Mon, Aug 14 - Sat, Aug 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ovie Carroll

Who Should Attend

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

"This course has a ton of excellent information. I have encountered some discussions in previous trainings but this shows practical application and how to find it."

-Cy Bleistine,
New Jersey State Police

SANS Technology Institute
www.sans.edu

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

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

FOR500: Windows Forensic Analysis (Formerly FOR408) focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook describes the tools and techniques that each investigator should use to solve a forensic case.

MASTER WINDOWS FORENSICS –
YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

Ovie Carroll *SANS Principal Instructor*

Ovie is the Director of the Cybercrime Lab of the Computer Crime and Intellectual Property Section (CCIPS) at the Department of Justice (DOJ). The lab provides advanced computer forensics, cybercrime investigation, and other technical assistance to DOJ prosecutors to support implementation of the department's national strategies for digital evidence and to combat electronic penetration, data theft, and cyberattacks on critical information systems. He also teaches two classes as an adjunct professor at George Washington University in Washington, DC. Prior to joining the DOJ, Ovie was a special agent in charge overseeing the Technical Crimes Unit of the Postal Inspector General's Office, where he was responsible for all computer intrusion investigations within the postal service network infrastructure and providing all digital forensic analyses in support of criminal investigations and audits. He also served as a special agent in the Air Force Office of Special Investigations, investigating computer intrusions and working both general crimes and counterintelligence, as well as conducting investigations into offenses including murder, rape, fraud, bribery, theft, and gangs and narcotics. **@ovie**

MGT414

SANS Training Program for CISSP® Certification

GISP Certification
Information Security Professional

www.giac.org/gisp

Six-Day Program
Mon, Aug 14 - Sat, Aug 19
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

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

www.sans.org/8140

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

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**

"Best security training I have ever received and just the right amount of detail for each domain."
-Tony Barnes, United States Sugar Corporation

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experiential knowledge in examples and explanations."
-Sean Hoar, Davis Wright Tremaine

"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

David R. Miller *SANS Certified Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information system security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs through policy writing; network architecture design (including security zones); the development of incident response teams and programs; the design and implementation of public key infrastructures; security awareness training programs; specific security solution designs, such as secure remote access and strong authentication architectures; disaster recovery planning and business continuity planning; and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer, and technical editor of books, curricula, certification exams, and computer-based training videos. **@DRM_CyberDude**

MGT514

GIAC CERTIFICATION COMING SOON!

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, Aug 14 - Fri, Aug 18
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

"I moved into management a few years ago and am currently working on a new security strategy/ roadmap and this class just condensed the past two months of my life into a one-week course and I still learned a lot!"

-Travis Evans, SiriusXM

SANS Technology Institute
www.sans.edu

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

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

• **Develop Strategic Plans**
Strategic planning is hard for people in IT and IT security, because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

• **Create Effective Information Security Policy**
Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that!"? Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

• **Develop Management and Leadership Skills**
Leadership is a capability that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities they can carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course, you will have the fundamental skills to create strategic plans to protect your company, enable key innovations, and work effectively with your business partners.

G. Mark Hardy *SANS Principal Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote who has spoken at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/ Information Security Advanced Technology Education Center of the National Science Foundation. Mr. Hardy is a retired U.S. Navy captain and was entrusted with nine command assignments, including responsibility for leadership training for 70,000 Sailors. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, a masters in business administration, a masters in strategic studies, and holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

ICS410

ICS/SCADA Security Essentials

GICSP Certification
Industrial Cyber Security Professional
www.giac.org/gicsp

Five-Day Program
Mon, Aug 14 - Fri, Aug 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Justin Searle

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

"Great introduction into ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company."
-Mike Poulos, Coca-Cola Enterprises

SANS Technology Institute
www.sans.edu

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

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

The course will provide you with:

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

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

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.

Justin Searle *SANS Senior Instructor*

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. He co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in international technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT). @meeas

Bonus Sessions

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

KEYNOTE: Current and Future Trends in Digital Investigative Analysis

Ovie Carroll

In this fun and fast-paced presentation, Ovie Carroll will discuss current and future trends in digital investigative analysis. The presentation will cover critical challenges faced by digital investigative analysts (computer forensic examiners) and discuss some of the most interesting digital artifacts.

State of the Dark Web

Matt Edmondson

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

Control Things Platform

Justin Searle

SamuraiSTFU was a great start to help electricity utilities do penetration testing of their DCS and SCADA networks, but it just wasn't enough. SamuraiSTFU has expanded its goals to include all control systems and IoT devices, thus requiring a name change and a complete rebuild of the pentest distribution. Come check out the new Control Things Platform, a pentesting platform to help you learn, calibrate, and perform security testing of control networks in any ICS organization.

Enhance Your Training Experience

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

SPECIAL PRICING

Extend Your Training Experience with an OnDemand Bundle

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

"The course content and OnDemand delivery method have both exceeded my expectations."
-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certifications

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

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

MORE INFORMATION

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

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

SANS Training Formats

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

Live Classroom Instruction

Premier Training Events

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

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

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

Summits

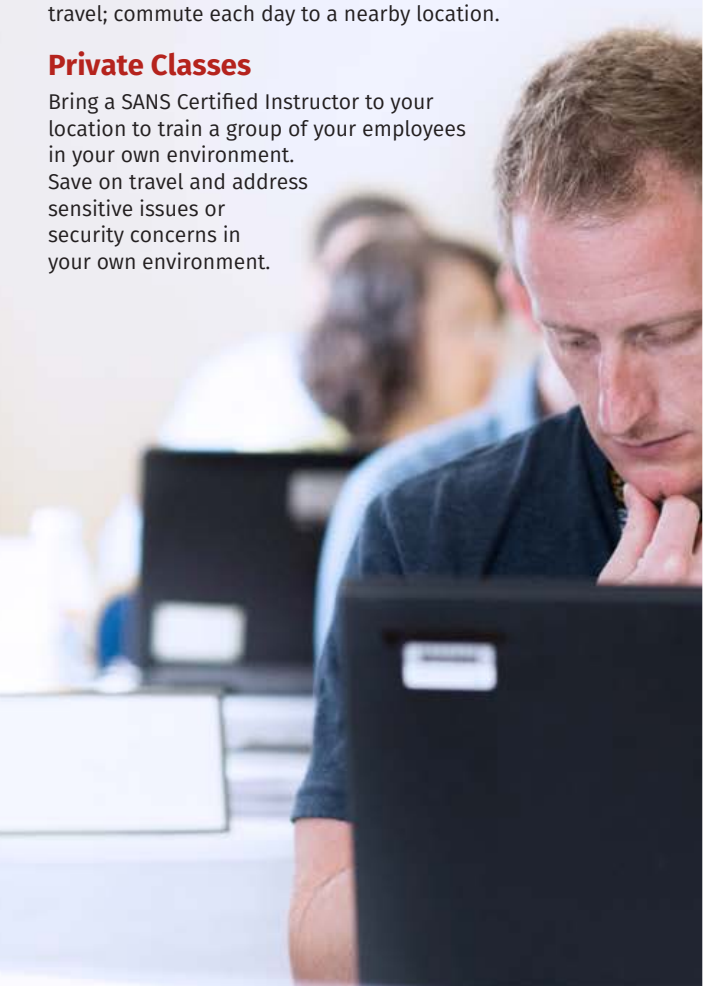
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

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

Private Classes

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



Online Training

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

Top reasons to take SANS courses online:

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

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

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

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

Future Training Events

Houston	Houston, TX	June 5-10
San Francisco Summer	San Francisco, CA	June 5-10
Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia	Columbia, MD	June 26 - July 1
Los Angeles – Long Beach	Long Beach, CA	July 10-15

SANSFIRE Washington, DC July 22-29

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

Network Security Las Vegas, NV Sep 10-17

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

Future Summit Events

Security Operations Center	Washington, DC	June 5-12
Digital Forensics	Austin, TX	June 22-29
ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5

Future Community SANS Events

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

Hotel Information

Sheraton Salt Lake City Hotel
150 West 500 South
Salt Lake City, UT 84101
Phone: 801-401-2000
www.sans.org/event/salt-lake-city-2017/location

Sheraton Salt Lake City Hotel is perfectly located in the heart of the downtown business and entertainment district and three blocks from the Salt Palace Convention Center. Whether you want to visit Temple Square, cheer on your favorite team, or shop at City Creek Mall, you'll find them all within walking distance of this downtown hotel or via the complimentary downtown TRAX.

Special Hotel Rates Available

A special discounted rate of $134.00 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 **July 21, 2017**. To make reservations, please call **888-627-8152** and ask for the SANS group rate.

Top 5 reasons to stay at the Sheraton Salt Lake City Hotel

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 Sheraton Salt Lake City Hotel, 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 Sheraton Salt Lake City Hotel that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/salt-lake-city**

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

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**6-21-17**	**$400.00**	**7-12-17**	**$200.00**

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

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **July 26, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

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

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

www.sans.org/account