SANS

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

SAN DIEGO 2017

October 30 - November 4

Protect Your Business and Advance Your Career

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

- CYBER DEFENSE
- ETHICAL HACKING
- PENETRATION TESTING
- CRITICAL SECURITY CONTROLS
- SECURITY OPERATIONS MANAGEMENT
- ICS/SCADA SECURITY
- SIEM

GIAC CERTIFICATIONS

CYBER DEFENSE NETWARS TOURNAMENT

SAVE $400

Register and pay by Sept 6th – Use code **EarlyBird17**

"SANS does an excellent job of keeping its training up to date. The labs really drive the material home."

-THERESA MENZEL, VERIZON

www.sans.org/san-diego

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 San Diego 2017 lineup of instructors includes:

Eric Conrad
Senior Instructor
@eric_conrad

Tim Conway
Certified Instructor

Christopher Crowley
Principal Instructor
@CCrowMontance

Matt Edmondson
Instructor
@matt0177

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Jonathan Ham
Certified Instructor
@jhamcorp

G. Mark Hardy
Principal Instructor
@g_mark

Seth Misenar
Senior Instructor
@sethmisenar

Greg Porter
Instructor

Bryan Simon
Certified Instructor
@BryanOnSecurity

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 13.

KEYNOTE: ***Actionable Detects: Blue Team Cyber Defense Tactics*** – Seth Misenar

State of the Dark Web – Matt Edmondson

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

Introducing DeepBlueCLI: A PowerShell Module for Hunt Teaming via Windows Event Logs – Eric Conrad

Save $400 when you register and pay by September 6th using code EarlyBird17

Courses at a Glance

	MON 10-30	TUE 10-31	WED 11-1	THU 11-2	FRI 11-3	SAT 11-4
SEC401 Security Essentials Bootcamp Style	Page 2 SIMULCAST					
SEC503 Intrusion Detection In-Depth	NEW! Page 3 SIMULCAST					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4					
SEC511 Continuous Monitoring and Security Operations	Page 5 SIMULCAST					
SEC555 SIEM with Tactical Analytics	NEW! Page 6					
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	Page 7					
MGT414 SANS Training Program for CISSP® Certification	Page 8					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 9					
MGT517 Managing Security Operations: Detection, Response, and Intelligence	NEW! Page 10					
ICS456 Essentials for NERC Critical Infrastructure Protection	Page 11					

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, Oct 30 - Sat, Nov 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

Who Should Attend

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

"This course has been invaluable in refreshing my networking, Windows, and security knowledge."

-Ron Mason, SLT Expressway

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

Also Available Via Simulcast
See page 17 for details.

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. **@BryanOnSecurity**

SEC503

Intrusion Detection In-Depth *NEW!*

GCIA Certification
Certified Intrusion Analyst
www.giac.org/gcia

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Kevin Fiscus

Who Should Attend

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

"The threats to our businesses and government agencies are ever increasing. We need to focus our IDS/IPS on our critical data and SEC503 helps us achieve that."
-Ed Brewster, SAIC Inc.

See page 17 for details.

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

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

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access to alerts and the ability to examine them in order to give them meaning and context. You will learn to investigate and reconstruct activity to determine if it is noteworthy or a false indication.

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

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian


www.sans.org/8140

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

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. He currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS's most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414. **@kevinbfiscus**

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler

www.giac.org/gcih

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
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

"SEC504 is an excellent course that ties the pieces of the incident handling and penetration testing puzzles together."
-Jonathon C., CACI

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

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

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

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

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

Matt Edmondson *SANS Instructor*

Matt performs technical duties for the U.S. government and is a principal at Argelius Labs, where he performs security assessments and consulting work. Matt's extensive experience with digital forensics includes conducting numerous examinations and testifying as an expert witness on multiple occasions. A recognized expert in his field with a knack for communicating complicated technical issues to non-technical personnel, Matt routinely provides cybersecurity instruction to individuals from the Department of Defense, Department of Justice, Department of Homeland Security, Department of 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**

SEC511

Continuous Monitoring and Security Operations

GMON Certification
Continuous Monitoring
www.giac.org/gmon

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Eric Conrad

Who Should Attend

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

"This course has been awesome at teaching me how to use tools and existing architecture in ways I haven't thought of before!"
-John Hubbard, GlaxoSmithKline

ALSO AVAILABLE VIA SIMULCAST
See page 17 for details.

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

"Keep on giving real-life scenarios to spice up the class. This class was perfect."
-Genevieve Opaye-Tetteh, eProcess Int SA

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

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

SANS Technology Institute
www.sans.edu

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

Eric Conrad *SANS Senior Instructor*

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

SEC555

SIEM with Tactical Analytics *NEW!*

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Seth Misenar

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Security monitoring personnel
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring or Network
- Individuals working in a hunt team capacity

"This course was uniquely valuable to me because my two companies don't have SIEMs – we have been proposing implementing them for years. You have saved me and my companies a lot of time and resources with this class! Thank you!"

-Dale Seefeldt, Rennes Group

Many organizations have logging capabilities but lack the people and processes to analyze logging systems. These systems collect vast amounts of data from a variety of sources, so proper analysis requires an understanding of those data sources. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. The class will also provide an understanding of the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK – a SANS-sponsored free Security Incident and Events Management (SIEM) solution – to provide the hands-on experience and mindset needed for large-scale data analysis.

Today, security operations do not suffer from a "big data" problem but rather a "data analysis" problem. Let's face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Add to this the daunting challenge that there is an infinite list of systems from which one can collect logs. It is easy to get lost in the perils of data saturation. This class is the switch from the typical churn-and-burn log systems to achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the appropriate use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the data are collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

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 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, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. **@sethmisenar**

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

GCCC Certification
Critical Controls

www.giac.org/gccc

Five-Day Program
Mon, Oct 30 - Fri, Nov 3
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Greg Porter

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

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

-Duane Harper, Community Health Systems

SANS Technology Institute
www.sans.edu

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

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS's in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

Greg Porter *SANS Instructor*

Greg Porter has both led and delivered comprehensive assessment activities that monitor, test, and audit the effectiveness of information system security controls. For the past several years, he has assisted organizations across the health care spectrum, ranging from integrated health care providers and community hospitals, to biotech and pharmaceutical organizations. Greg is also the founder of Allegheny Digital, an information security consultancy specializing in enterprise risk management, incident response, and threat monitoring. Greg graduated from the University of Pittsburgh, received his master's degrees from Carnegie Mellon University, and holds a number of professional certifications.

MGT414

SANS Training Program for CISSP® Certification

GISP Certification
Information Security Professional

www.giac.org/gisp

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
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: Jonathan Ham

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**

"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 in 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

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small start-ups to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the Cyber Incident Response Team for one of the largest U.S. civilian federal agencies. He has held the CISSP, GSEC, GCIA, and GCIH certifications and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. **@jhamcorp**

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, Oct 30 - Fri, Nov 3
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

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

"I have some very specific, achievable things I can do right away suggested by the course that will benefit my organization and me. That's valuable training."

-William E. Weyandt, American Orthodontics

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.

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!

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

G. Mark Hardy *SANS Principal Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events worldwide. 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. He 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, and a masters in strategic studies, and holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

MGT517

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

Five-Day Program
Mon, Oct 30 - Fri, Nov 3
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

Who Should Attend

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

"Wow! Chris is wicked smart, knows this space, and is a real expert. It would be very hard to do better or have a more solid presentation."

-Michael Carter, LDS Church

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

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

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

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

Course Author Statement

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

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

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

-Christopher Crowley

Christopher Crowley *SANS Principal Instructor*

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

ICS456

Essentials for NERC Critical Infrastructure Protection

GCIP Certification
Critical Infrastructure Protection

www.giac.org/gcip

Five-Day Program
Mon, Oct 30 - Fri, Nov 3
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Tim Conway

Who Should Attend

- IT and OT (ICS) cybersecurity professionals
- Field support personnel
- Security operations personnel
- Incident response personnel
- Compliance staff
- Team leaders
- Governance officials
- Vendors/Integrators
- Auditors

This course empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and the Regional entities. It provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. The course also covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance. Our 25 hands-on labs range from securing workstations to digital forensics and lock picking.

Course Day Descriptions

456.1 HANDS ON: Asset Identification and Governance

A transition is under way from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. On day 1 students will develop an understanding of the electricity sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls. The day will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition that helps bring the concepts to life and highlights the important role we play in defending the grid.

456.2 HANDS ON: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. During day 2 we move beyond the "what" of CIP compliance to understanding the "why" and the "how." Firewalls, proxies, gateways, IDS and more – learn where and when they help and learn practical implementations to consider and designs to avoid. Physical protections include more than fences and you'll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce what is learned throughout the day and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

456.3 HANDS ON: System Management

CIP-007 has consistently been one of the most violated Standards going back to CIP version 1. With the CIP Standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day 3, students will dive into CIP-007. We'll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. This day will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We'll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

456.4 HANDS ON: Information Protection and Response

Education is key to every organization's success with NERC CIP and the students in ICS 456 will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, all students can be a valued resource to their organization's CIP-004 training program, the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. On day 4 we'll examine CIP-008 and CIP-009 covering identification, classification, and communication of incidents as well as the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs will introduce tools for ensuring file integrity and sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

456.5 HANDS ON: CIP Process

On the final day students will learn the key components for running an effective CIP Compliance program. We will review the NERC processes for standards development, violation penalty determination, Requests For Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally we'll identify recurring and audit-related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFEs, and self-reporting. We'll also look at the challenge of preparing for NERC audits and provide tips to be prepared to demonstrate the awesome work your team is doing. Finally, we'll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of day 5 students will have a strong call to action to participate in the ongoing development of CIP within their organization and in the industry overall as well as a sense that CIP is do-able! Labs will cover DOE C2M2, audit tools, and an audit-focused take on the "blue team – red team" exercise.

Tim Conway *SANS Certified Instructor*

Tim is the technical director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He previously served as the director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim was also an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He was the chair of the RFC CIPC, and is the current chair of the NERC CIP Interpretation Drafting Team, a member of the NESCO advisory board, chair of the NERC CIPC GridEx Working Group, and chair of the NBISE Smart Grid Cyber Security panel.

CYBER DEFENSE NETWARS TOURNAMENT

Test your cybersecurity knowledge and skills LIVE at

SANS San Diego 2017 with 2 free nights of NetWars!

NOVEMBER 2 & 3 **6:30-9:30 PM**

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. **REGISTRATION FOR NETWARS IS FREE OF CHARGE TO ALL STUDENTS AT SANS SAN DIEGO 2017.** External participants are welcome to join for an entry fee of $1,520.

The all-new NetWars Defense Competition is a defense-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. With so much focus on offense, NetWars Defense is a truly unique experience and opportunity to test your skills in architecture, operations, threat hunting, log analysis, packet analysis, cryptography, and much more!

Who Should Attend

- System administrators
- Enterprise defenders
- Architects
- Network engineers
- Incident responders
- Security operations specialists
- Security analysts
- Security auditors
- Builders and breakers

sans.org/san-diego

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: Actionable Detects: Blue Team Cyber Defense Tactics

Seth Misenar

Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration. Seth Misenar's ever-evolving Actionable Detects presentations provide you with the understanding, tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

State of the Dark Web

Matt Edmondson

Have you heard people talk about the dark web for the past few years and wondered what all the fuss was about? Maybe you've even fired up TOR and visited an .onion site or two for "research." Well if you want to take your dark web knowledge from moderate to cromulent, this is the presentation for you! 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.

Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

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

Introducing DeepBlueCLI: A PowerShell Module for Hunt Teaming via Windows Event Logs

Eric Conrad

A number of events are triggered in Windows environments during virtually every successful breach. These include service creation events and errors, user creation events, extremely long command lines, compressed and base64 encoded PowerShell functions, and more. Microsoft has added a wealth of blue team tools to its operating systems, including native support of logging the full command line used to launch all processes, without requiring third-party tools (or Sysmon). KB3004375 adds this feature to Windows 7 and Server 2008R2. DeepBlueCLI can automatically determine events that are typically triggered during most successful breaches, including use of malicious command lines including PowerShell.

SANS

Enhance Your **Training Experience**

Special Pricing

Add an **OnDemand Bundle** & **GIAC Certification Attempt***

to your course within seven days of this event for just **$689** each.

Price goes up to $729 Oct 1st

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

"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's 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 D.C., 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 16 for upcoming training events in North America.

Summits

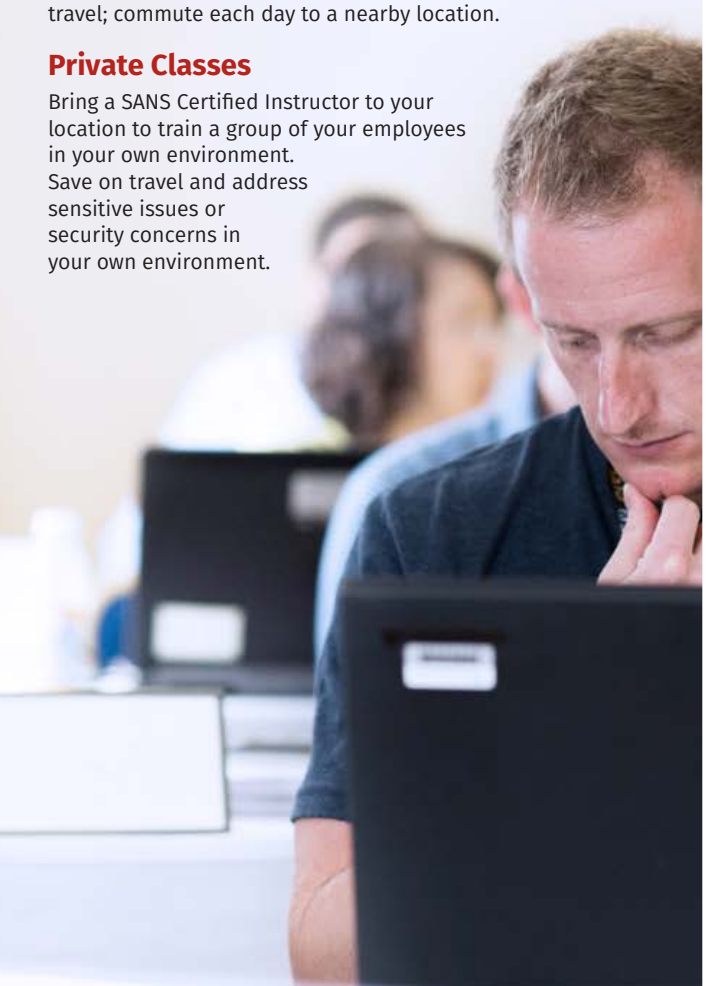
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs are 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

New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security Las Vegas, NV Sep 10-17

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

Cyber Defense Initiative Washington, DC Dec 12-19

Security East New Orleans, LA Jan 8-13, 2018

Northern Virginia Winter	Reston, VA	Jan 15-20
Las Vegas	Las Vegas, NV	Jan 28 - Feb 2
Miami	Miami, FL	Jan 29 - Feb 3
Scottsdale	Scottsdale, AZ	Feb 5-10
Southern California – Anaheim	Anaheim, CA	Feb 12-17
Dallas	Dallas, TX	Feb 19-24

Future Summit Events

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
Cyber Threat Intelligence	Washington, DC	Jan 27 - Feb 6, 2018

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

Hard Rock Hotel San Diego

207 Fifth Avenue (Corner of Fifth & L St.)
San Diego, CA 92101
Phone: 619-702-3000
www.sans.org/event/san-diego-2017/location

There's something electric about being in the middle of it all. Hard Rock Hotel San Diego puts you in the limelight with chic accommodations in the heart of downtown and the famed nightlife of the Gaslamp Quarter. And you can live it up without ever leaving the hotel – try a jam session in your suite with our complimentary Sound of Your Stay service, mouthwatering sushi at world-famous Nobu, and rooftop cocktails at Float rooftop lounge or 207 bar.

Special Hotel Rates Available

A special discounted rate of $235.00 S/D will be honored based on space availability.

The group rate includes high-speed Internet in your room and is only available through **October 2, 2017**. Government per diem rooms can only be secured by emailing Vanessa Mendiola at **vanessa.mendiola@hardrockhotelsd.com**. Vanessa will respond within 48 business hours. Please call **619-702-3000** and ask for the SANS rate to make a reservation.

Top 5 reasons to stay at the Hard Rock Hotel San Diego

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 Hard Rock Hotel San Diego, 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 Hard Rock Hotel San Diego that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

REGISTER ONLINE AT
www.sans.org/san-diego

WE RECOMMEND YOU REGISTER EARLY TO ENSURE YOU GET YOUR FIRST CHOICE OF COURSES.

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

SANS Simulcast

To register for a SANS San Diego 2017 Simulcast course, please visit **www.sans.org/event/san-diego-2017/attend-remotely**

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**9-6-17**	**$400.00**	**9-27-17**	**$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 **October 4, 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