SANS San Diego 2016

October 23-28

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

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Nine courses on

CYBER DEFENSE
PEN TESTING
SECURE OPERATIONS
APPLICATION SECURITY
CISSP® TRAINING

"SANS has enhanced my technical skills, but more importantly did so within a proper technology, risk, and business context."
-Scott Ramsey,
Reinalt-Thomas Corp.

GIAC-Approved Training

SAVE $400
when you register & pay by August 31st using code **EarlyBird2016**

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 2016 lineup of instructors includes:

Doc Blackburn
SANS Instructor
@DocBlackburn

Eric Conrad
Senior Instructor
@eric_conrad

Mick Douglas
SANS Instructor
@bettersafetynet

Jason Fossen
Faculty Fellow
@JasonFossen

Frank Kim
Certified Instructor
@sansappsec
@fykim

Seth Misenar
Senior Instructor
@sethmisenar

Keith Palmgren
Senior Instructor
@kpalmgren

Mike Poor
Senior Instructor
@Mike_Poor

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 10.

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

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

How to Build a Cybersecurity Platform the Easy Way – Keith Palmgren

Not a Single Dime! Just Say No To Ransomware – Mick Douglas

Advancing the Security Agenda: Compelling Leadership to Support Security
Doc Blackburn

Save $400 when you register and pay by August 31st using code EarlyBird2016

Courses-at-a-Glance

		SUN 10-23	MON 10-24	TUE 10-25	WED 10-26	THU 10-27	FRI 10-28
SEC301	Intro to Information Security	Page 1					
SEC401	Security Essentials Bootcamp Style	Page 2					
SEC501	Advanced Security Essentials – Enterprise Defender	Page 3					
SEC503	Intrusion Detection In-Depth	Page 4					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 5					
SEC505	Securing Windows and PowerShell Automation	Page 6					
SEC511	Continuous Monitoring and Security Operations	Page 7					
MGT414	SANS Training Program for CISSP® Certification	Page 8					
DEV541	Secure Coding in Java/JEE: Developing Defensible Apps	Page 9					

Denotes Simulcast is available for this course

SEC301:

Intro to Information Security

SANS

Five-Day Program
Sun, Oct 23 - Thu, Oct 27
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Doc Blackburn

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

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

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

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

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

"The course is excellent as is! Great flow from topic to topic."
-Danielle Alexander, Bechtel

www.giac.org/gisf

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

"The instructor was excellent and the basis for my new knowledge of computer cyber-crimes for law enforcement. This course will help with our investigation and detection of cyber-fraud in the field."
-Justine Killeen, NYPD

Doc Blackburn *SANS Instructor*

Doc Blackburn has over 30 years of experience in system and software design, server and network administration and website programming. His interest in computers started in 1982 when he first started programming in DOS on a Texas Instruments TI-99 4a and continued as a dedicated computer hobbyist until he decided to make information technology a full-time career in 1998. Doc ran a successful IT consulting, hosting, and design firm for 12 years until he found his passion was in systems security and compliance. His well-rounded experience includes hardware, software, network design, project management, administration, programming, systems security, and compliance frameworks. He has vast experience at various levels of information technology from technical support to security leadership roles. He has been heavily involved in the technical design and implementation of NIH-approved and FISMA-compliant information systems. His current work has focused on HIPAA, FERPA, PCI DSS, and FISMA compliant systems with an emphasis on IT risk management in enterprise environments. Doc holds the ITIL, CISSP, HCISPP (healthcare, HIPAA), PCI ISA (payment card industry) and GIAC GSEC, GISF, GPEN, GCPM, GCIA and GSLC certifications along with a bachelor's degree from the University of Arizona. He is currently the IT Compliance Administrator for the University of Colorado Denver/Anschutz Medical Campus. @DocBlackburn

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

www.sans.org/simulcast

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian


www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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

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

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

"This course has given me a great start on truly understanding the fundamentals of security and applying it." -John Houser, First Citizens Bank

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

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 11 GIAC certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. 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

SEC501:

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Keith Palmgren

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials – Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT – DETECT – RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

"This training will help me greatly to advance my career in a DoD IT cybersecurity position as an ISSO."
-Yvonne E. DoD AFN-BC

Of course, despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust prevention and detection measures, completing the security lifecycle.

"I recommend this course to anyone trying to develop valuable skills, and knowledge in security."
-Ivonne Cedillo, California Employment Development Department

ALSO AVAILABLE VIA SIMULCAST
www.sans.org/simulcast

GCED
www.giac.org/gced

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

Keith Palmgren *SANS Senior Instructor*

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

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Poor

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

Who Should Attend

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

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

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

"SEC503 directly covers the necessary knowledge and skill set I use every day at my job. The added insight is worth the price."
-Michael Garrett, Federal Reserve Bank of San Francisco

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

Also Available Via Simulcast
www.sans.org/simulcast

GCIA
www.giac.org/gcia

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

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

Mike Poor *SANS Senior Instructor*

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Mick Douglas

www.giac.org/gcih

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This was an extremely engaging course that highlights new ways of looking into incident response."
-Ryan Guest, Southern Company

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

"SEC504 teaches you methods for testing your defenses and how to identify weaknesses in your network and systems."
-Rene Graf, Federal Home Loan Bank

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

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

"This course provides an eye-opening overview of methods and tools used by bad actors as well as a good explanation of incident handling processes!"
-Steven J. Sparks, Honeywell

Mick Douglas *SANS Instructor*

Even when his job title indicated otherwise, Mick Douglas has been doing information security work for over 10 years. He received a bachelor's degree in communications from Ohio State University and holds the CISSP, GCIH, GPEN, GCUX, GWEB, and GSNA certifications. He currently works at Binary Defense Systems as the DFIR Practice Lead. He is always excited about an opportunity to share with others so they do not have to learn the hard way! Mick's teaching helps security professionals of all abilities gain useful tools and skills to make their jobs easier. When he's not "geeking out" you'll likely find Mick indulging in one of his numerous hobbies; photography, scuba diving, or hanging around in the great outdoors. @bettersafetynet

SEC505:
Securing Windows and PowerShell Automation

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and adaptive Windows security at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – *now what?* A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we'll never win, and we'll never get ahead of the game. By the time your Security Information and Event Manager (SIEM) or monitoring system tells you a Domain Admin account has been compromised, it's TOO LATE.

For the assume breach mindset, we must carefully delegate *limited* administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

Learning PowerShell is also useful for another kind of security: *job* security. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too. Besides, PowerShell is also simply fun to use.

This course is designed for systems engineers, security architects, and the SecOps team. The focus of the course is on how to automate those Windows-related Critical Security Controls that are the most effective, but also the most difficult to implement, especially in large environments.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don't cover patch management, share permissions, or other such basics – the aim is to go far beyond all that. Come have fun learning PowerShell and agile Windows security at the same time!

"This training was an excellent balance between theory and practical applications, extremely relevant to current trends, concepts, and technologies."
-Chris S., Naval Surface Warfare Center

Who Should Attend

- Security Operations (SecOps) engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure (PKI) or smart cards
- Anyone who needs to reduce malware infections

ALSO AVAILABLE VIA SIMULCAST
www.sans.org/simulcast

GCWN
www.giac.org/gcia

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

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

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. @JasonFossen

SEC511:
Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Eric Conrad

ALSO AVAILABLE VIA SIMULCAST
www.sans.org/simulcast

GMON
www.giac.org/gmon

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"SEC511 is a good technical overview of why we fail today and offers practical solutions to fix security issues we all face."
-Brad Milhorn, CompuCom

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

Who Should Attend

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

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

"This training is valuable because it helped me understand network security from various types of prevention and provided good insight into endpoint security."
-Stephen L. Perry, Ardent Health Services

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

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

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Sun, Oct 23 - Fri, Oct 28
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Seth Misenar

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2016 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

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.

Who Should Attend

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

You Will Be Able To:

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

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

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

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
www.sans.org/cissp

www.giac.org/gisp

www.sans.org/8140

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

"I would recommend this class for anyone wanting to get a CISSP. I feel it gave me the tools to be confident to take the test."
-Matthew Trummer, Lincoln Electric Systems

Seth Misenar *SANS Senior Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which 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 previously served as both physical and network security consultant for Fortune 100 companies and the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor's of science 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 CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

DEV541:

Secure Coding in Java/JEE: Developing Defensible Applications

SANS

Four-Day Program
Sun, Oct 23 - Wed, Oct 26
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Frank Kim

www.sans.org/simulcast

www.giac.org/gssp-java

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This training is so useful and necessary. There are not enough developers who get this kind of hybrid of high level concepts and hands-on learning. I know I will use almost everything we covered in my job.
-Emily Hillenbrand, XOR Security

This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- Identify security defects in your code
- Fix security bugs using secure coding techniques
- Utilize secure HTTP headers to prevent attacks
- Secure your sensitive representational state transfer (REST) services
- Incorporate security into your development process
- Use freely available security tools to test your applications

Who Should Attend

- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) programmers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a high-level theory course – it is about real-world, hands-on programming. You will examine actual code, work with real tools, build applications and gain confidence in the resources you need to improve the security of Java applications.

Rather than teaching students to use a given set of tools, the course covers concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques that you have learned in course.

Frank Kim *SANS Certified Instructor*

As CISO at the SANS Institute, Frank leads the security risk function for the most trusted source of computer security training, certification, and research in the world. He also helps shape, develop, and support the next generation of security leaders by teaching, developing courseware, and leading the management and software security curricula. Prior to the SANS Institute, Frank was Executive Director of Cyber Security at Kaiser Permanente with responsibility for delivering innovative security solutions to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business-enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is the author of popular SANS courseware on strategic planning, leadership, and application security. @sansappsec @fykim

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE: **Actionable Detects: Blue Team Cyber Defense Tactics**

Seth Misenar

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Eric Conrad

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

How To Build a Cybersecurity Platform the Easy Way

Keith Palmgren

Building a cybersecurity program is easy. Building a cybersecurity program that is effective is seriously hard! When faced with a seemingly insurmountable task, prioritization is vital. Investing time and money in the right place at the right time is the difference between success and being the next cyberbreach headline.

Whether you are new to cybersecurity or an old hand, you may feel lost in the storm. If so, this talk is for you. Cybersecurity's five historic and current pitfalls that prevent organizations from building an effective IT security platform will be discussed: poor passwords, vulnerabilities, malware/crimeware, insider threat, and mismanagement.

To build that effective cybersecurity platform in today's ever-changing information technology environment, organizations must prioritize and focus on five key principles that address those pitfalls. We must look at those critical security principles in new and different ways: The Principle of Least Privilege; Authentication, Authorization, and Accountability (AAA); Confidentiality, Integrity, and Availability (CIA); Policy, Procedure, and Training (PPT); Hardening, Patching, and Monitoring (HPM); and Protect, Detect, and Respond (PDR).

Every organization needs a cybersecurity strategy. An effective strategy requires that you understand the problems as well as the solutions to those problems. Only then can you prioritize your limited cybersecurity resources. Managers and technicians alike will gain valuable insight in this non-technical talk.

Not a Single Dime! Just Say No To Ransomware

Mick Douglas

By taking several steps to lower costs, organizations of any size can greatly reduce the impact ransomware has on an organization. This talk will teach you how to detect and respond faster to this all too common threat.

Advancing the Security Agenda: Compelling Leadership to Support Security

Doc Blackburn

Are you having trouble convincing the decision-makers in your business to support security initiatives? Are your concerns being ignored? You are not alone! One of the biggest challenges InfoSec professionals face today is getting leadership to support their activities. There have been many recent cases of security not getting enough resources until after a breach. Unfortunately, many times, the security team is shown the door after the breach because it was considered their fault. Don't let this happen to you. You know what to do, and how to do it. You know how important it is to your organization. The technology exists to fix your concerns. So, why won't leadership fund it? Find out how to gain support for your activities and receive the support your security initiatives need.

Enhance Your Training Experience

WITH:

Even More Training Value

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 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 Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- 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

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Portland 2016
Portland, OR | Aug 8-13

Dallas 2016
Dallas, TX | Aug 8-13

DEV531: **Defending Mobile Apps**
San Francisco, CA | Aug 8-9

DEV534: **Secure DevOps**
San Francisco, CA | Aug 10-11

Data Breach SUMMIT
Chicago, IL | Aug 18

Chicago 2016
Chicago, IL | Aug 22-27

Alaska 2016
Anchorage, AK | Aug 22-27

Virginia Beach 2016
Virginia Beach, VA | Aug 22 - Sep 2

NORTHERN VIRGINIA **Crystal City** 2016
Crystal City, VA | Sep 6-11

Network Security 2016
Las Vegas, NV | Sep 10-19

Security Leadership
SUMMIT & TRAINING 2016
Dallas, TX | Sep 27 - Oct 4

Seattle 2016
Seattle, WA | Oct 3-8

Baltimore 2016
Baltimore, MD | Oct 10-15

Tysons Corner 2016
Tysons Corner, VA | Oct 22-29

Pen Test Hackfest
SUMMIT & TRAINING 2016
Crystal City, VA | Nov 2-9

Information on all events can be found at
www.sans.org/security-training/by-location/all

SANS SAN DIEGO 2016

Hotel Information

Training Campus
Hard Rock Hotel

207 Fifth Avenue
San Diego, CA 92101 | 619-702-3000
www.sans.org/event/san-diego-2016/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 just steps from downtown and the famed nightlife of the Gaslamp Quarter. The Hard Rock's award-winning service and stunning event venues amp up any occasion. And you can live it up without ever leaving the hotel.

Special Hotel Rates Available

A special discounted rate of $229.00 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. This rate is only available through Monday, September 26, 2016.

Top 5 reasons to stay at the Hard Rock 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 Hard Rock 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 Hard Rock Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN DIEGO 2016

Registration Information

We recommend you register early to ensure you get the course of your choice.

Register online at www.sans.org/san-diego

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 **EarlyBird16** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**8-31-16**	**$400.00**	**9-21-16**	**$200.00**

Some restrictions apply.

SANS SIMULCAST

To register for a SANS San Diego 2016 Simulcast course, please visit www.sans.org/event/san-diego-2016/attend-remotely

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

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by October 5, 2016 – processing fees may apply.