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

SANS Dallas 2017

February 27 – March 4

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Eight courses on

Cyber Defense

Penetration Testing

Incident Response

Ethical Hacking

Management

"The knowledge I am learning from SANS training can be implemented immediately."

-Keiva Rhodes, SAIC

GIAC
GIAC-Approved Training

SAVE $400

Register and pay by Jan 4th – Use code **EarlyBird17**

www.sans.org/dallas

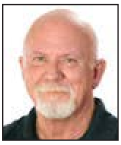
SANS Instructors

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 Dallas 2017 lineup of instructors includes:

Adrien de Beaupre
Certified Instructor
@adriendb

Jason Fossen
Faculty Fellow
@JasonFossen

G. Mark Hardy
Certified Instructor
@g_mark



Paul A. Henry
Senior Instructor
@phenrycissp

David R. Miller
Certified Instructor
@DRM_CyberDude

Bryan Simon
Certified Instructor
@BryanOnSecurity

Matthew Toussain
SANS Instructor
@0sm0s1z

Ismael Valenzuela
SANS Instructor
@aboutsecurity

Evening Bonus Sessions

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

KEYNOTE: ***What's New for Security in Windows Server 2016 and Windows 10?***
Jason Fossen

HTTPdeux
Adrien de Beaupre

How to Commit Card Fraud
G. Mark Hardy

Save $400 when you register and pay by Jan 4th using code EarlyBird17

Courses-at-a-Glance

		MON 2-27	TUE 2-28	WED 3-1	THU 3-2	FRI 3-3	SAT 3-4
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC501	Advanced Security Essentials - Enterprise Defender	Page 2					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC505	Securing Windows and PowerShell Automation	Page 4					
SEC511	Continuous Monitoring and Security Operations	Page 5					
SEC560	Network Penetration Testing and Ethical Hacking	Page 6					
MGT414	SANS Training Program for CISSP® Certification	Page 7					
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	Page 8					

Register today for SANS Dallas 2017!
www.sans.org/dallas

@SANSInstitute
Join the conversation:
#SANSDallas

SEC401:
Security Essentials Bootcamp Style

Six-Day Program
Mon, Feb 27 - Sat, Mar 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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.

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 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

www.giac.org/gsec

www.sans.edu

www.sans.org/8140

www.sans.org/cyber-guardian

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

"Loved this course! So practical. My customer's systems will be more secure as a result of this course."
-Howard Foster, Schneider Electric

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 12 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. 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

Six-Day Program
Mon, Feb 27 - Sat, Mar 4
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Paul A. Henry

GIAC CERTIFIED ENTERPRISE DEFENDER
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

"Paul Henry is an excellent instructor who presents large volumes of information effectively."
-Rowley Molina, Altria

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

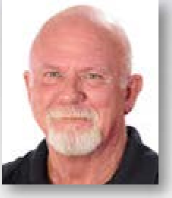
- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

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.



Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. @phenrycissp

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Feb 27 - Sat, Mar 4
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor:
Adrien de Beaupre

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

Who Should Attend

- Incident handlers
- 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 instructor's depth of knowledge, his attitude, and his communication skills are phenomenal." -Greg Witt, ICBC

This course enables you to turn the tables on computer attackers by helping you to 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 gets you into the attacker's mindset and thinking like the attacker. Now you know what to defend from."
-Cameron Pollock, IBM

GCIH
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

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

SANS

SEC505:

Securing Windows and PowerShell Automation

Six-Day Program
Mon, Feb 27 - Sat, Mar 4
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. PowerShell is free and open source on GitHub for Linux and Mac OS, too.

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 the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement 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 is a really great course for anyone involved in administration or securing of windows environments."-David Hazar, Oracle

Who Should Attend

- Security Operations (SecOps) engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- 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

GCWN
www.giac.org/gcwn

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

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
Mon, Feb 27 - Sat, Mar 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Ismael Valenzuela

GMON
www.giac.org/gmon

SANS Technology Institute
www.sans.edu

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

"This course had great lessons that will be actionable to what I do day to day, and it will help me fill in the gaps at my current work environment."
-Kevin South, Navient Corporation

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.

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 course has provided me with a great deal of food for thought for my enterprise."
-Mike Bubb, Mitre Corporation

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.

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

Ismael Valenzuela *SANS Instructor*

Since he founded one of the first IT Security consultancies in Spain, Ismael Valenzuela has participated as a security professional in numerous projects across the globe over the past 15 years. He currently works as IR/Forensics Technical Practice Manager at Intel Security in North America. Prior to joining Intel, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world's largest providers of healthcare IT solutions. He holds a bachelor's degree in computer science from the University of Malaga (Spain), is certified in business administration, and holds many professional certifications including the highly regarded GIAC Security Expert (GSE #132) in addition to GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, CISSP, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK. Some of his articles are freely available at http://blog.ismaelvalenzuela.com. @aboutsecurity

SANS

SEC560: Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Feb 27 - Sat, Mar 4
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Matthew Toussain

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

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

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

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. **You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.**

Who Should Attend

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

GPEN
www.giac.org/gpen

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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

"Learning how attackers profile and exploit allows me to understand how to tailor our product offerings to provide real value."
-Travis Smith, Tripwire

Matthew Toussain *SANS Instructor*

Matthew Toussain is an active-duty Air Force officer and the founder of Spectrum Information Security, a firm focused on maximizing the value proposition of information security programs. As an avid information security researcher, Matthew regularly hunts for vulnerabilities in computer systems and releases tools to demonstrate the effectiveness of attacks and countermeasures. He has been a guest speaker at many conference venues, including DEFCON, the largest security conference in the world. After graduating from the U.S. Air Force Academy, where he architected and instructed the summer cyber course that now trains over 400 cadets per year, Matthew served as the Senior Cyber Tactics Development Lead for the U.S. Air Force. He directed the teams responsible for developing innovative Tactics, Techniques, and Procedures for offensive operations as well as for cyber protection teams (CPT). Later, as a member of the 688th Cyber Warfare Wing he managed the Air Force's transition of all 18 CPTs to fully operational capability. As a founding member of Spectrum, Matthew regularly performs a wide variety of information security services. He earned his master's degree in information security engineering as one of the first graduates of the SANS Technology Institute and supports many national and international cyber competitions including the CCDC, Netwars, and the National Security Agency's Cyber Defense Exercise as a red team member and instructor. @0sm0s1z

MGT414:
SANS Training Program for CISSP® Certification

Six-Day Program
Mon, Feb 27 - Sat, Mar 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: David R. Miller

SANS

GISP
www.giac.org/gisp

www.sans.org/8140

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

> "The instructor was excellent and truly an expert! I'm getting depth in my understanding and David explained some topics better than several books I've read."
> -Freda Lurdy, Raytheon

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.

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 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 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

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.

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

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

David R. Miller *SANS Certified Instructor*

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

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, Feb 27 - Fri, Mar 3
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

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 learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. In addition, 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.

Who Should Attend

- All newly appointed information security officers
- Technically-skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what their technical people are telling them

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

GSLC
www.giac.org/gslc

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

> "Mark Hardy has excellent teaching skills, and keeps all material interesting using real-life examples. His talk on crypto was awesome!"
> -Brett Todé, Zoetis

G. Mark Hardy *SANS Certified 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 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for InfoSec, public key infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he has bachelor's degrees in computer science and mathematics, and master's degrees in business administration and strategic studies, along with the GSLC, CISSP, CISM, and CISA certifications. @g_mark

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:

What's New for Security in Windows Server 2016 and Windows 10?

Jason Fossen

In this lively talk, Jason Fossen, author of the Securing Windows and PowerShell Automation (SEC505) course at SANS, will lay out what's new for security in Windows 10 and Windows Server 2016, such as Credential Guard and Windows as a Service (WaaS). He will also talk about some of the epic changes going on at Microsoft now that CEO Steve Ballmer is gone, such as open-source PowerShell for Linux and Mac OS. Is it really a new era for Microsoft? Come join the presentation and see what Microsoft is betting its future on!

HTTPDeux

Adrien de Beaupre

This talk will discuss the relatively newly approved and published HTTP/2 protocol. The agenda will include reasons why the new protocol was developed, how it is implemented, tools that can use it, and challenges it presents to penetration testers.

How to Commit Card Fraud

G. Mark Hardy

Well, we're not going to show you how to commit fraud, but we will show you how the bad guys do it and how you can protect yourself and your business.

We'll take a look into the "dark web" and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over $16 billion annually. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet.

Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

Enhance Your Training Experience

Add an

OnDemand Bundle & **GIAC Certification Attempt***

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

SPECIAL PRICING

Extend Your Training Experience with an OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

GIAC

Get Certified with GIAC Certification

- 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

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

Cyber Defense Initiative 2016
Washington, DC | Dec 10-17

Security East 2017
New Orleans, LA | Jan 9-14

Las Vegas 2017
Las Vegas, NV | Jan 23-30

Cyber Threat Intelligence
SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

SOUTHERN CALIFORNIA
Anaheim 2017
Anaheim, CA | Feb 6-11

Scottsdale 2017
Scottsdale, AZ | Feb 20-25

San Jose 2017
San Jose, CA | Mar 6-11

Tysons Corner Spring 2017
McLean, VA | Mar 20-25

ICS Security
SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27

Pen Test Austin 2017
Austin, TX | Mar 27 - Apr 1

SANS 2017
Orlando, FL | Apr 7-14

Threat Hunting and IR
SUMMIT & TRAINING 2017
Orlando, FL | Apr 18-25

Baltimore Spring 2017
Baltimore, MD | Apr 24-29

Automotive Cybersecurity
SUMMIT & TRAINING 2017
Detroit, MI | May 1-8

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

SANS DALLAS 2017

Hotel Information

Training Campus

The Westin Dallas Downtown

1201 Main Street
Dallas, TX 75202
972-584-6650
www.sans.org/event/dallas-2017/location

Located in vibrant downtown Dallas next to Belo Garden and a mile from the Kay Bailey Convention Center, The Westin Dallas Downtown puts you in the center of it all. This hotel is located within a mile of Klyde Warren Park, the Perot Museum of Nature and Science, and the American Airlines Center.

Special Hotel Rates Available

A special discounted rate of $182.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through February 6, 2017.

Top 5 reasons to stay at The Westin Dallas Downtown

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 Westin Dallas Downtown, 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 Westin Dallas Downtown that you won't want to miss!
5. Everything is in one convenient location!

SANS DALLAS 2017

Registration Information

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

Register online at www.sans.org/dallas

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.

Use code **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**1-4-17**	**$400.00**	**1-25-17**	**$200.00**

Some restrictions apply.

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 February 8, 2017 – processing fees may 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