

SANS

NORTHERN VIRGINIA
Tysons Corner 2016

October 22-29

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

10 courses on
CYBER DEFENSE
PEN TESTING
DIGITAL FORENSICS
SECURITY MANAGEMENT
IT AUDIT

"As always with
SANS courses, there
is a lot of great
material!"

-LIBBY H.,
ARMY RESEARCH
LABORATORY



**SAVE
\$400**

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

www.sans.org/tysons-corner

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 Tysons Corner 2016 lineup of instructors includes:



Dr. Eric Cole
Faculty Fellow
@drrericcole



G. Mark Hardy
Certified Instructor
@g_mark



Paul A. Henry
Senior Instructor
@phenrycissp



Randy Marchany
Certified Instructor
@randymarchany



David R. Miller
Certified Instructor
@DRM_CyberDude



Chris Pizor
Certified Instructor
@chris_pizor



Clay Risenhoover
Certified Instructor



Lance Spitzner
Certified Instructor
@lspitzner



Alissa Torres
Certified Instructor
@sibertor

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 10.

KEYNOTE: *Evolving Threats* – Paul A. Henry

How to Commit Card Fraud – G. Mark Hardy

The “Know Normal, Find Evil” Series: Windows 10 Memory Forensics Overview
Alissa Torres

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

Courses-at-a-Glance

		SAT 10-22	SUN 10-23	MON 10-24	TUE 10-25	WED 10-26	THU 10-27	FRI 10-28	SAT 10-29
SEC401	Security Essentials Bootcamp Style			Page 1					
SEC440	Critical Security Controls: Planning, Implementing, and Auditing		Page 9						
SEC501	Advanced Security Essentials – Enterprise Defender			Page 2					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling			Page 3					
SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception			Page 4					
FOR508	Advanced Digital Forensics and Incident Response			Page 5					
MGT414	SANS Training Program for CISSP® Certification			Page 6					
MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program		Page 9						
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™			Page 7					
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems			Page 8					

Register today for SANS Tysons Corner 2016!

www.sans.org/tysons-corner



@SANSInstitute
Join the conversation:
#SANSTysons

Security Essentials Bootcamp Style

Six-Day Program

Mon, Oct 24 - Sat, Oct 29

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Dr. Eric Cole


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

"I received the best
explanation of crypto ever.

Great job Dr. Cole!"

-AARON A.,

(NAVSEA) CDSA DAM NECK

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.

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



Dr. Eric Cole SANS Faculty Fellow

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is the founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drericcole

SEC501:

Advanced Security Essentials – Enterprise Defender

Six-Day Program

Mon, Oct 24 - Sat, Oct 29

9:00am - 5:00pm

Laptop Required

36 CPEs

Instructor: Paul A. Henry



www.giac.org/gced



www.sans.edu



www.sans.org/8140



**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

**“SEC501 is a must
for cybersecurity
professionals!”**

-GARY OAKLEY,

**BECHTEL MARINE PROPULSION
CORPORATION**



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

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.

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.

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

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Oct 24 - Sat, Oct 29
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Staff



www.giac.org/gcih



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

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

Author Statement

"One of my greatest joys in life is helping people understand the complex landscape of security so that they can implement really effective defenses. It may be difficult to fully grasp what truly impacts the security of your organization versus what is simply product marketing hype. This class is the nexus between attacks and defenses, chock full of vital information for thwarting today's nastiest attacks. Ed Skoudis and I continuously refine this class based on the multitude of penetration tests we conduct and incidents we handle regularly. We strive to keep the material relevant, interesting, and directly applicable to the job of infosec professionals. And I personally live for the moments when the light goes on within a SEC504 student and they finally see through the noise and begin to understand what is important from a threat and vulnerability perspective."

-John Strand

Active Defense, Offensive Countermeasures & Cyber Deception

Five-Day Program
Mon, Oct 24 - Fri, Oct 28
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Chris Pizor

"SEC550 is the next step in the evolution of cyber defense in learning to make the hackers' job harder, track their movements, and get attribution."

-MICK LEACH, NATIONWIDE

"SEC550 was great training, and very helpful to better understand analysis, offensive security, and also how to improve the protection."

-STEFANIA IANNELLI,

PALO ALTO NETWORKS



Chris Pizor SANS Certified Instructor

Chris Pizor is a civilian employee working for the U.S. Air Force as the lead curriculum designer for cyber warfare operations training. Chris served on active duty in the U.S. Air Force as a Network Intelligence Analyst before retiring in 2010. He was part of the initial cadre of the National Security Agency Threat Operations Center and helped develop tactics to discover and eradicate intrusions into U.S. government systems. Chris has worked for 20 years in the intelligence community, with 12 years focused on cybersecurity. Over the course of his active duty career, Chris received multiple individual and team awards. Chris is passionate about security and helping others advance their security knowledge. He is continuously researching and refining his own skills so he can prepare U.S. airman and other professionals to defend their vital networks and critical infrastructure. Chris earned a bachelor's degree in intelligence studies and information operations, and is pursuing a master's degree in cybersecurity. He holds the GSEC, GCIA, GCIH, GPEN, GXPN, and GCFA certifications. @chris_pizor

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550:Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

Who Should Attend

- ▶ General security practitioners
- ▶ Penetration testers
- ▶ Ethical hackers
- ▶ Web application developers
- ▶ Website designers and architects

You Will Be Able To

- ▶ Track bad guys with callback Word documents
- ▶ Use Honeybadger to track web attackers
- ▶ Block attackers from successfully attacking servers with honeypots
- ▶ Block web attackers from automatically discovering pages and input fields
- ▶ Understand the legal limits and restrictions of Active Defense
- ▶ Obfuscate DNS entries
- ▶ Create non-attributable Active Defense Servers
- ▶ Combine geolocation with existing Java applications
- ▶ Create online social media profiles for cyber deception
- ▶ Easily create and deploy honeypots

What You Will Receive

- ▶ A fully functioning Active Defense Harbinger Distribution ready to deploy
- ▶ Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments

FOR508:

Advanced Digital Forensics and Incident Response

Six-Day Program

Mon, Oct 24 - Sat, Oct 29

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Alissa Torres



www.giac.org/gcfa



www.sans.edu



www.sans.org/cyber-guardian



www.sans.org/8140



**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"Great material and instructor, the lab scenarios were very well done and fun to investigate." -BRYAN THIRY, LOCKHEED MARTIN



Alissa Torres SANS Certified Instructor

Alissa Torres specializes in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security spanning government, academic, and corporate environments and holds a bachelor's degree from the University of Virginia and a master's from the University of Maryland in information technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCPE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+ certifications. @sibertor

SANS

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occurred
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An advanced persistent threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

"I liked the focus on doing the things that matter most in an incident response, and I learned a lot during time-line labs about the importance of knowing how the timesharing is modified." -NIKLAS ANDERSSON, CORESEC SYSTEMS

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

SANS Training Program for CISSP® Certification

Six-Day Program

Mon, Oct 24 - Sat, Oct 29
 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



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

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.

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

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

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.**

<https://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 to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs like 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

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program

Mon, Oct 24 - Fri, Oct 28

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPEs

Laptop NOT Needed

Instructor: G. Mark Hardy


www.giac.org/gslc

www.sans.edu

www.sans.org/8140

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"Mark is a wealth of knowledge and experience which adds value to the class. His injection of real-world scenarios as he is teaching is very helpful."

-PAM L., NATIONAL NUCLEAR
SECURITY ADMINISTRATION



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

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.

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!

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

AUD 507:

Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program

Mon, Oct 24 - Sat, Oct 29

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Clay Risenhoover


www.giac.org/gsna

www.sans.edu

www.sans.org/8140

**BUNDLE
ONDEMAND**

WITH THIS COURSE

www.sans.org/ondemand

"This course not only prepares you to perform a comprehensive audit, but also provides excellent information for operations to improve network security posture."

-RIFAT IKRAM, STATE DEPT. FCU



Clay Risenhoover SANS Certified Instructor

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay's experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sectors. He has a master's degree in computer science and holds a number of technical and security certifications, including the GPEN, GSNA, CISA, CISM, GWEB, and CISSP.

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise.

What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

"AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!" -CARLOS E., U.S. ARMY

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are and why. Sign up for this course and experience the mix of theory, hands-on, and practical knowledge.

Who Should Attend

- ▶ Auditors seeking to identify key controls in IT systems
- ▶ Audit professionals looking for technical details on auditing
- ▶ Managers responsible for overseeing the work of an audit or security team
- ▶ Security professionals newly tasked with audit responsibilities
- ▶ System and network administrators seeking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- ▶ System and network administrators seeking to create strong change control management and detection systems for the enterprise

SECURITY SKILL-BASED COURSE

SEC440

Critical Security Controls: Planning, Implementing, and Auditing

Two-Day Course | Sat, Oct 22 - Sun, Oct 23 | 12 CPEs | Laptop NOT Needed | Instructor: Randy Marchany

This course will help you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). The controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. The controls were selected and defined by the U.S. military, other government agencies (including the NSA, DHS, GAO, and many others), and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. These entities defined the controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented.

"The information in this course is usable on day one back at the office." -PETER SEGALINI, PEPSICO

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

You will find the full document describing the Critical Security Controls posted at the Center for Internet Security at www.cisecurity.org/critical-controls.cfm.

MANAGEMENT SKILL-BASED COURSE

MGT433

Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program

Two-Day Course | Sat, Oct 22 - Sun, Oct 23 | 12 CPEs | Laptop NOT Needed | Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain, and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers as well. Please bring example materials from your security awareness program that you can show and share with other students during the course.

Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

"This is very valuable training — particularly for those that have not had any experience with putting together a security awareness training program."

-JAMES POMEROV, SEIM JOHNSON LL



www.sans.edu

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:

Evolving Threats

Paul A. Henry

For nearly two decades, defenders have fallen into the “crowd mentality trap.” They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and on attempting to outwit an attacker’s delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and \$157 billion in data breach costs in only the past six years. This presentation will highlight recent and current developments in the evolution of both attacks and defenses.

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.

The “Know Normal, Find Evil” Series: Windows 10 Memory Forensics Overview

Alissa Torres

It’s time to re-up your skills at hunting evil in memory by learning the new normal, Windows 10. Advance your memory forensics skills for what is expected to be the most rapidly adopted enterprise Windows version of all time. Find out what is new in Windows 10 OS artifacts, browsing history, and memory management and how the memory forensic frameworks are keeping up. With a current adoption rate of 15% and growing, it is only a matter of time before this OS version will make up the majority of your digital forensics and incident response casework. This presentation will provide insight into the significant changes introduced with Windows 10 and how they will affect your investigative process.

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

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

NORTHERN VIRGINIA Crystal City 2016

Crystal City, VA | Sep 6-11

Dallas 2016

Dallas, TX | Aug 8-13

Network Security 2016

Las Vegas, NV | Sep 10-19

DEV531: Defending Mobile Apps

San Francisco, CA | Aug 8-9

Security Leadership SUMMIT & TRAINING 2016

Dallas, TX | Sep 27 - Oct 4

DEV534: Secure DevOps

San Francisco, CA | Aug 10-11

Seattle 2016

Seattle, WA | Oct 3-8

Data Breach SUMMIT

Chicago, IL | Aug 18

Baltimore 2016

Baltimore, MD | Oct 10-15

Chicago 2016

Chicago, IL | Aug 22-27

San Diego 2016

San Diego, CA | Oct 23-28

Alaska 2016

Anchorage, AK | Aug 22-27

Pen Test Hackfest SUMMIT & TRAINING 2016

Crystal City, VA | Nov 2-9

Virginia Beach 2016

Virginia Beach, VA | Aug 22 - Sep 2

Information on all events can be found at

www.sans.org/security-training/by-location/all

Hotel Information

Training Campus
Hilton McLean Tysons Corner

7920 Jones Branch Drive
McLean, VA 22102 | 703-847-5000
www.sans.org/event/tysons-corner-2016/location

The Hilton McLean Tysons Corner hotel is ideally located minutes from the Ronald Reagan National Airport and the Washington Dulles International Airport. Guest rooms in this nine-story hotel feature thoughtful amenities for work and relaxation. Dine in the contemporary härth restaurant with fireside dining, serving American cuisine cooked in a wood-burning oven. Enjoy handcrafted cocktails and regional beers in the adjacent härth bar.

Special Hotel Rates Available

A special discounted rate of \$204.00 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 Friday, September 30, 2016.

Top 5 reasons to stay at the Hilton McLean Tysons Corner

- 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 Hilton McLean Tysons Corner 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 Hilton McLean Tysons Corner that you won't want to miss!
- 5 Everything is in one convenient location!

SANS TYSONS CORNER 2016

Registration Information

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



Register online at www.sans.org/tysons-corner

Select your course or courses 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 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.

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/security-resources