THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS

Capital Region

FALL 2015

Crystal City 2015

September 8-13

Baltimore 2015

September 21-26

Tysons Corner 2015

October 12-17

Save $400

Register & pay early! See page 21 for more details.

SEC301:
Intro to Information Security

SEC401:
Security Essentials Bootcamp Style

SEC501:
Advanced Security Essentials – Enterprise Defender

SEC503:
Intrusion Detection In-Depth

SEC504:
Hacker Tools, Techniques, Exploits, and Incident Handling

SEC550:
Active Defense, Offensive Countermeasures and Cyber Deception

SEC566:
Implementing and Auditing the Critical Security Controls – In-Depth

FOR408:
Windows Forensic Analysis

FOR508:
Advanced Digital Forensics and Incident Response

FOR526:
Memory Forensics In-Depth

FOR585:
Advanced Smartphone Forensics

MGT414:
SANS Training Program for CISSP® Certification

MGT512:
SANS Security Leadership Essentials For Managers with Knowledge Compression™

MGT514:
IT Security Strategic Planning, Policy, and Leadership

AUD507:
Auditing & Monitoring Networks, Perimeters, and Systems

ICS410:
ICS/SCADA Security Essentials

SANS Capital Region FALL 2015

	Crystal City Crystal City, VA September 8-13 sans.org/crystalcity #SANSCrystalCity	**Baltimore** Baltimore, MD September 21-26 sans.org/baltimore #SANSBaltimore	**Tysons Corner** Tysons Corner, VA October 12-17 sans.org/tysonscorner #SANSTysonsCorner
SEC301: Intro to Information Security	**SEC301**		
SEC401: Security Essentials Bootcamp Style	**SEC401**	**SEC401**	**SEC401**
SEC501: Advanced Security Essentials – Enterprise Defender			**SEC501**
SEC503: Intrusion Detection In-Depth		**SEC503**	**SEC503**
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	**SEC504**	**SEC504**	**SEC504**
NEW! **SEC550:** Active Defense, Offensive Countermeasures, and Cyber Deception		**SEC550**	
SEC566: Implementing and Auditing the Critical Security Controls – In-Depth	**SEC566**		
FOR408: Windows Forensic Analysis	**FOR408**		
FOR508: Advanced Digital Forensics and Incident Response			**FOR508**
FOR526: Memory Forensics In-Depth		**FOR526**	
FOR585: Advanced Smartphone Forensics			**FOR585**
MGT414: SANS Training Program for CISSP® Certification			**MGT414**
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™	**MGT512**		
MGT514: IT Security Strategic Planning, Policy & Leadership			**MGT514**
AUD507: Auditing & Monitoring Networks, Perimeters, and Systems	**AUD507**		
ICS410: ICS/SCADA Security Essentials	**ICS410**		

TRAINING EVENTS:

Crystal City
September 8-12
Instructor:
Keith Palmgren

SANS
SEC301

Five-Day Program
30 CPEs
Laptop Required

YOU WILL BE ABLE TO:

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Gain an understanding of computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies including anti-malware, firewalls, and intrusion detection systems.
- Determine your "SPAM IQ" to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Have an introductory level of knowledge regarding incident response, business continuity, and disaster recover planning
- Install and use the following tools: Password Safe, Secunia PSI, Malwarebytes, and Syncback

SEC301
Intro to Information Security

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

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

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

"If you are just starting out in information security, this course has all the basics needed to get you started."
-Sherrie Audrict, Deltha Corporation

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

"This class is great for IT professionals looking for their first step towards security awareness. I have been in IT for 17 years and I learned a lot on this first day of class."
-Paul Beninati, EMC

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

GIAC INFORMATION SECURITY FUNDAMENTALS GISF
giac.org

▶❚❚ **Bundle OnDemand**
WITH THIS COURSE
sans.org/ondemand

SEC401

Security Essentials Bootcamp Style

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.

STOP and ask yourself the following questions:

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

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

> *"SEC401 is the best InfoSec training bar none. The value for the money is unbeatable!"* -Ron Foupht, Sirius Computer Solutions

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

GIAC Security Essentials Certification GSEC
giac.org

SANS Technology Institute
sans.edu

supere aude
sans.org/cyber-guardian

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

TRAINING EVENTS:

Crystal City
September 8-13
Instructor:
Tim Garcia

Baltimore
September 21-26
Instructor:
Paul A. Henry

Tysons Corner
October 12-17
Instructor:
Bryan Simon

SANS

SEC401

Six-Day Program
46 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

Tysons Corner
October 12-17
Instructor:
Keith Palmgren

SANS

SEC501

Six-Day Program
36 CPEs
Laptop Required

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

SEC501
Advanced Security Essentials – Enterprise Defender

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.

> *"I enjoyed real-life business cases that were discussed in SEC501 to make the material relevant."*
> -Lorelei Duff, Lockheed Martin

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.

> *"Very knowledgeable. Top-tier training and industry leading."*
> -Herbert Monford, Regions Bank

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.

> *"After taking SEC401 and GSEC, this course is the perfect follow up, going deep into attacking techniques while understanding the most-used vulnerabilities and how to defend your network against those attacks."*
> -Fawaz AlHomoud, Saudi Aramco

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 preventive and detective measures, completing the security lifecycle.

GCED
giac.org

SANS Technology Institute
sans.edu

▶❚❚ **Bundle OnDemand** with this course
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

SEC503
Intrusion Detection In-Depth

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

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

"Today has been brilliant, bringing all of our skills together to achieve the challenge. I wish we could do this every day!"

-Hayley Roberts, MOD

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

"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."

-Thomas Kelly, DIA

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

GCIA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org
/cyber-guardian

▶II
Bundle OnDemand
with this course
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS

sans.org/8570

TRAINING EVENTS:

Baltimore
September 21-26
Instructor:
Jonathan Ham

Tysons Corner
October 12-17
Instructor:
Johannes Ullrich, PhD

SANS
SEC503

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

Crystal City
September 8-13
Instructor:
Kevin Fiscus

Baltimore
September 21-26
Instructor:
Adrien de Beaupre

Tysons Corner
October 12-17
Instructor:
Michael Murr

SANS
SEC504

Six-Day Program
37 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling

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.

> *"The instructor opened my eyes and helped me understand how to approach the concepts of offensive security and incident handling. He is one of the very best."*
> -Stephen Ellis, CB&I

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, detect, and respond to them. 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. It will enable you to discover the holes in your system before the bad guys do!

> *"Our organization has incident response pieces all over. This course is valuable in putting the pieces together and improving the plan and, more importantly, the mindset."*
> -Tyler Burwitz, TEEX

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.

GIAC CERTIFIED INCIDENT HANDLER GCIH
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

SEC550
Active Defense, Offensive Countermeasures, and Cyber Deception

NEW

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.

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 honeyports
- 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

Author Statement

I wrote this course to finally make defense fun, to finally add some confusion to the attackers, and to change the way we all look at defense. One of the most frequent questions I get is why offensive countermeasures are so important. Many people tell me that we cannot ignore patching, firewalls, policies, and other security management techniques. I cannot agree more. The techniques presented in this course are intended for organizations that have gone through the process of doing things correctly and want to go further. Get your house in order, and then play. Of course, there will be challenges for anyone trying to implement offensive countermeasures in their organization. However, they can all be faced and overcome.
- John Strand

TRAINING EVENTS:

Baltimore
September 21-25
Instructor:
Bryce Galbraith

SANS

SEC550

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Security professionals and systems administrators who are tired of playing catch-up with attackers
- Anyone who is in IT and/or security and wants defense to be fun again

TRAINING EVENTS:

Crystal City
September 8-12
Instructor:
Randy Marchany

SANS

SEC566

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

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

"The 20 controls presented in the course are requirements found in most regulated industries. I found the format and layout of each control well explained and easy to follow." -Josh Ellis, Iberdrola USA

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

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

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

- **Create a strategy to successfully defend their data**
- **Implement controls to prevent data from being compromised**
- **Audit systems to ensure compliance with Critical Control standards.**

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

giac.org

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

FOR408
Windows Forensic Analysis

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

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

"I have been doing forensic investigations for several years, but would highly recommend this course (FOR408) for both new and old forensic investigations." -Robert Galarza, JP Morgan Chase

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook,). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out - attendees learn to analyze everything from legacy Windows XP systems to just discovered Windows 8.1 artifacts.

FOR408 is continually updated: This course utilizes a brand-new intellectual property theft and corporate espionage case that took over 6 months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator can encounter while analyzing Windows systems. The incredibly detailed workbook details the tools and techniques step-by-step that each investigator should follow to solve a forensic case.

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

GIAC CERTIFIED FORENSIC EXAMINER GCFE

giac.org

SANS Technology Institute

sans.edu

▶❚❚ BUNDLE ONDEMAND WITH THIS COURSE

sans.org/ondemand

TRAINING EVENTS:

Crystal City
September 8-13
Instructor:
Mike Pilkington

SANS
FOR408

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

DFIR
digital-forensics.sans.org

TRAINING EVENTS:

Tysons Corner
October 12-17
Instructor:
Jake Williams

SANS

FOR508

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Information security professionals
- Incident response team leaders and members
- Security Operations Center (SOC) personnel
- System administrators
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

DFIR
digital-forensics.sans.org

FOR508
Advanced Digital Forensics and Incident Response

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

- How the breach occured
- Compromised and affected systems
- What attackers took or changed
- Incident containment and remediation

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.

> *"FOR508 is an extremely valuable course overall. It brings essential topics into one class and covers an extensive amount of topics along with excellent reference material."*
> -Edgar Zayas, U.S. Securities and Exchange Commission

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.

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.

> *"FOR508 has been the best DFIR course I've taken so far. All the material is recent and it shows a lot of time went into the material."*
> -Louise Cheung, Stroz Friedberg

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, the incident response course (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 – TIME TO GO HUNTING!

GCFA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

FOR526
Memory Forensics In-Depth

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

> *"The training opened my eyes for the need to collect memory images as well as physical images for single computer analysis such as theft of IP or other employee investigations."*
>
> -Greg Caouette, Kroll

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526: Memory Forensics in-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture to ensure data integrity and combat anti-acquisition techniques.
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms.
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low-level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior.
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques, as well as how to devise custom parsing scripts for targeted memory analysis.

MALWARE CAN HIDE, BUT IT MUST RUN.

TRAINING EVENTS:

Baltimore
September 21-26
Instructor:
Alissa Torres

SANS
FOR526

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Incident response team members
- Experienced digital forensic analysts
- Red team members
- Penetration testers
- Exploit developers
- Law enforcement officers
- Federal agents or detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

DFIR
digital-forensics.sans.org

Course updates, prerequisites, special notes, or laptop requirements: **sans.org/courses**

TRAINING EVENTS:

Tysons Corner
October 12-17
Instructor:
Heather Mahalik

SANS

FOR585

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Experienced digital forensics examiners
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, or detectives
- IT auditors
- Graduates of SANS SEC575, FOR408, FOR508, or FOR518 who want to take their skills to the next level

DFIR
digital-forensics.sans.org

FOR585
Advanced Smartphone Forensics

It is almost impossible today to conduct a digital forensic investigation that does not include a smartphone or mobile device. Smartphones are replacing the need for a personal computer, and almost everyone owns at least one. The smartphone may be the only source of digital evidence tracing an individual's movements and motives, and thus can provide the who, what, when, where, why, and how behind a case. FOR585: Advanced Smartphone Forensics teaches real-life, hands-on skills that help digital forensic examiners, law enforcement officers, and information security professionals handle investigations involving even the most complex smartphones currently available.

"FOR585 course content is extremely valuable for use in real-world application and directly pertinent to analysis conducted at my lab. It's great to go to a class and be able to utilize nearly everything that was taught."
-H. Polend, Virginia Dept. of Forensic Science

The course focuses on smartphones as sources of evidence, providing students with the skills needed to handle mobile devices in a forensically sound manner, manipulate locked devices, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. Students will walk away with knowledge they can immediately put to use on their next smartphone investigation.

The hands-on exercises in this course cover the best commercial and open-source tools available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization with the capability to use evidence from smartphones.

"The topics covered in the course can be considered advanced but are also very practical. Topics such as parsing and searching devices not supported by commercial tools and digging in hex for deleted artifacts are extremely important."
-Matthew Edmondson

This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and constantly changing, most forensics professionals are unfamiliar with the data formats. It is time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU!

▶❚❚
Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

MGT414
SANS Training Program for CISSP® Certification

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

> *"I think the course material and the instructor are very relevant for the task of getting a CISSP. The overall academic exercise is solid."*
>
> -Aaron Lewter, Availity

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

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

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)^2 that form a critical part of 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 8 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 8 domains of knowledge
- Apply the skills learned across the 8 domains to solve security problems when you return to work

You Will Receive With This Course:

- Course books for each of the 8 domains
- 320 questions to test knowledge and preparation for each domain

**Note: CISSP® exams are not hosted by SANS.
You will need to make separate
arrangements to take the CISSP® exam.**

Take advantage of SANS' CISSP® Get Certified Program currently being offered.
sans.org/special/cissp-get-certified-program

giac.org

▶II **Bundle OnDemand** WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS

sans.org/8570

Course updates, prerequisites, special notes, or laptop requirements: **sans.org/courses**

TRAINING EVENTS:

Tysons Corner
October 12-17
Instructor:
David R. Miller

Course Updated
for New CISSP® Exam

SANS
MGT414

Six-Day Program
46 CPEs
Laptop NOT Needed

WHO SHOULD ATTEND:

- Security professionals who are interested in understanding 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 the eight domains of knowledge can be applied to their current job

MGT512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

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. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

> *"MGT512 is awesome! Lots of material covered, so I will need to go back and read the notes and study more. The course was very structured, relevant, and concise."* -Juan Canino, SWIFT

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!

GIAC Security Leadership Certification GSLC
giac.org

SANS Technology Institute
sans.edu

▶II
Bundle OnDemand
with this course
sans.org/ondemand

Meets DoDD 8570 Requirements
sans.org/8570

Training Events:

Crystal City
September 8-12
Instructor:
G. Mark Hardy

SANS

MGT512

Five-Day Program
33 CPEs
Laptop NOT Needed

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

MGT514
IT Security Strategic Planning, Policy, and Leadership

As security professionals we have seen the landscape change. Cyber security is now more vital, crucial, relevant, and important to the growth of your organization than ever before. As a result, information security teams have more budget and more opportunity. With this increased responsibility comes more scrutiny. Security business leaders must learn how to navigate in this new world of security.

This course teaches security professionals how to do three things:

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal.

Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, case scenarios, team based exercises, and discussions that put students in real-world scenarios you will experience activities that you can conduct with your own team members at work.

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

TRAINING EVENTS:

Tysons Corner
October 12-16
Instructors:
Frank Kim,
Mark Williams

SANS
MGT514

Five-Day Program
30 CPEs
Laptop NOT Needed

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

Crystal City
September 8-13
Instructor:
Clay Risenhoover

SANS

AUD507

Six-Day Program
36 CPEs
Laptop Required

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 looking 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

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems

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 will be given from real-world examples.

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 how to automatically validate defenses through instrumentation and automation of audit checklists.

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

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

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 theoretical, hands-on, and practical knowledge.

GSNA
giac.org

SANS Technology Institute
sans.edu

▶II
Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

ICS410
ICS/SCADA Security Essentials

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

The course will provide you with:

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

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

"ICS410 really opens you up to possibilities and issues that otherwise you wouldn't really think about." -Alfonso Barreiro, Panama Canal Authority

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

GICSP
giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

TRAINING EVENTS:

Crystal City
September 8-12
Instructor:
Graham Speake

SANS
ICS410

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of computer based training modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.

SANS SECURING THE HUMAN

For a free trial, visit us at
securingthehuman.org

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training!
OnDemand Bundles are just $629
when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- Labs
- MP3s and Videos of lectures
- Subject-Matter Expert support

Visit sans.org/ondemand/bundles
for more information about OnDemand Bundles now.

FUTURE SANS TRAINING EVENTS

SANS Capital City 2015
Washington, DC | July 6-11 | #SANSDC

SANS Digital Forensics & Incident Response SUMMIT & TRAINING
Austin, TX | July 7-14 | #DFIRSummit

SANS San Jose 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS Minneapolis 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS Boston 2015
Boston, MA | August 3-8 | #SANSBoston

SANS Cyber Defense SUMMIT & TRAINING
Nashville, TN | August 11-18 | #CyberDefenseSummit

SANS San Antonio 2015
San Antonio, TX | August 17-22 | #SANSSATX

SANS Security Awareness SUMMIT & TRAINING
Philadelphia, PA | August 17-25 | #SecAwareSummit

SANS Virginia Beach 2015
Virginia Beach, VA | August 24 - September 4 | #SANSVaBeach

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events 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 sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

HOTEL INFORMATION

CRYSTAL CITY 2015

Training Campus
DoubleTree by Hilton
Washington DC-Crystal City

300 Army Navy Drive
Arlington, VA 22202

sans.org/event/crystal-city-2015/location

Special Hotel Rates Available

A special discounted rate of $159.00 S/D will be honored based on space availability.
Government per diem rooms may be 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 August 15, 2015.

BALTIMORE 2015

Training Campus
Hilton Baltimore

401 West Pratt Street
Baltimore, MD 21201

sans.org/event/baltimore-2015/location

Special Hotel Rates Available

A special discounted rate of $189.00 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 August 31, 2015.

TYSONS CORNER 2015

Training Campus
Hilton McLean Tysons Corner

7920 Jones Branch Drive
McLean, VA 22102

sans.org/event/tysons-corner-2015/location

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability.
Government per diem rooms may be 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 Sept. 21, 2015.

REGISTRATION INFORMATION

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

Register online at:

CRYSTAL CITY:	**sans.org/event/crystal-city-2015/courses**
BALTIMORE:	**sans.org/event/baltimore-2015/courses**
TYSONS CORNER:	**sans.org/event/tysons-corner-2015/courses**

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.

Use code
EarlyBird15
when registering early

Pay Early and Save

	EVENT	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	Crystal City	7/15/15	$400.00	8/12/15	$200.00
	Baltimore	7/29/15	$400.00	8/26/15	$200.00
	Tysons Corner	8/19/15	$400.00	9/16/15	$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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 respective dates (see website for dates) – processing fees may apply.