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

INFORMATION SECURITY TRAINING

Baltimore
Fall 2018
September 8-15

Protect Your Business | Advance Your Career

Thirteen hands-on, immersion-style courses taught by real-world practitioners

See inside for courses offered in:

- Cyber Defense
- Penetration Testing
- Digital Forensics
- Security Management
- Monitoring and Detection
- Audit

PLUS NEW COURSES

- Open-Source Intelligence Gathering and Analysis
- Defensible Security Architecture
- SIEM Design & Implementation
- Measuring and Managing Cyber Risk Using FAIR

“The hands-on, real-world application throughout this training allowed for a deeper understanding of how our networks can be attacked and how they should be defended. SANS is by far the best InfoSec training available in the world!”

- Brian Bailey, West Virginia State Treasurer’s Office

SAVE $400
Register and pay by July 18th
Use code EarlyBird18

www.sans.org/baltimore-fall
SANS Instructors
Fewer than 100 individuals are currently qualified and designated to teach as SANS Instructors worldwide. This select group of professionals includes recognized industry experts and real-world practitioners, all of whom have proven to be engaging teachers in the classroom. Their up-to-date examples and deep knowledge ensure that what you learn in class will be relevant to your job.
For instructor bios, visit: www.sans.org/instructors
The line-up of SANS Instructors for SANS Baltimore Fall 2018 includes:

Ted Demopoulos
Principal Instructor
@TedDemop

Kevin Fiscus
Principal Instructor
@kevinbfiscus

Bryce Galbraith
Principal Instructor
@brycegalbraith

G. Mark Hardy
Principal Instructor
@g_mark

Justin Henderson
Certified Instructor
@SecurityMapper

Micah Hoffman
Certified Instructor
@WebBreacher

David R. Miller
Certified Instructor
@DRM_CyberDude

David Musselwhite
Instructor

Kevin Ripa
Instructor
@kevinripa

Clay Risenhoover
Certified Instructor
@AuditClay

Bryan Simon
Certified Instructor
@BryanOnSecurity

Jake Williams
Senior Instructor
@MalwareJake

Evening Bonus Sessions
Take advantage of these extra evening presentations and add more value to your training. Learn more on page 15.

Courses at a Glance

SEC301 Introduction to Cyber Security
SEC401 Security Essentials Bootcamp Style
SEC455 SIEM Design & Implementation
SEC487 Open-Source Intelligence Gathering and Analysis
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling
SEC511 Continuous Monitoring and Security Operations
SEC530 Defensible Security Architecture
SEC560 Network Penetration Testing and Ethical Hacking
FOR500 Windows Forensic Analysis
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
MG512 SANS Security Leadership Essentials for Managers with Knowledge Compression™
AUD507 Auditing & Monitoring Networks, Perimeters, and Systems
HOSTED Measuring and Managing Cyber Risk Using FAIR

Save $400 when you register and pay by July 18th using code EarlyBird18
Register today for SANS Baltimore Fall 2018!
www.sans.org/baltimore-fall
Extend and Validate Your Training

Add an OnDemand Bundle OR GIAC Certification Attempt to your course within seven days of this event to get bundle pricing.*

Extend Your Training Experience with an OnDemand Bundle

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

OnDemand Bundle price – $729

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

- ROBERT JONES, Team Jones, Inc.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

GIAC bundle price – $729

“GIAC is the only certification that proves you have hands-on technical skills.”

- CHRISTINA FORD, DEPARTMENT OF COMMERCE

More Information

www.sans.org/ondemand/bundles | www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

▐ Do you have basic computer knowledge, but are new to cybersecurity 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 cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301. This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you.

You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come. 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 SANS course in this progression, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

“"The course provided me with a lot of great information from the low to the high levels in several areas. A lot of the concepts are something I will be able to use in my day-to-day job.””

- Sandy Baguskas, Sandy Baguskas

David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs. 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 David has worked on 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.
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.edu/institute

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

Ted Demopoulos
SANS Principal Instructor
@TedDemop

Ted Demopoulos’ first significant exposure to computers was in 1977 when he had unlimited access to his high school’s PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a 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.

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.

Is SEC401: Security Essentials Bootcamp Style the right course for you? 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, then the SEC401 course will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our course will show you how to prevent your organization’s security problems from being headline news in the Wall Street Journal! Prevention is ideal but detection is a must.

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

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

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.
Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their efforts to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide excellent solutions to his customers. Micah holds GIAC’s GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP®. Micah is an active member of the NoVAHackers community, writes Recon-ng modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on the Appalachian Trail or the many park trails in Maryland.
The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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

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

“SEC504 is foundational and core strength-building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both the adversary and defender.”

- Araceli Ari Gomes, Dell Secureworks

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12 years. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GFCA-Gold, GCIA-Gold, GCIH, GAWN, GPMA, GCWN, GCSC-Gold, GSEC, SC5A, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. He has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS’s most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414.
SEC511: Continuous Monitoring and Security Operations

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

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

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

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!
Architecture is designed to help students build and maintain a truly defensible security architecture. “The perimeter is dead” is a favorite saying in this age of mobile, cloud, and the Internet of Things. We are indeed living in a new world of “de-perimeterization” where the old boundaries of “inside” and “outside” or “trusted” and “untrusted” no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the “encrypt everything” mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of how to build and maintain up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better prevent the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

You Will Learn To:

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Maximize the current investment by reconfiguring existing equipment to become more defensible
- Configure computer systems and network components to support proper logging and continuous monitoring
- Improve both preventive and detective capabilities
- Improve the security of devices from layer 1 (physical) through layer 7 (application)

Justin Henderson is a passionate and dedicated information technology professional who has been in the field since 2005. Justin focuses on providing comprehensive industry training and uses his knowledge and experience to mentor others. Justin is particularly proficient in working with technical platforms, including operating systems, networking, security, storage, and virtualization, but he has also worked in governance, project management, and service management. He has a BS degree in network design and administration from Western Governors University and has over 40 certifications, including the GPEN and GCWN. Justin has also taught network security at Lake Land College. Some of his other achievements include mentoring individuals in the information technology field as well as developing the virtual dojo, a fully automated cloud computing solution showcase environment.
As a cybersecurity professional, you have a unique responsibility to find and understand your organization’s vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 is the must-have course for every well-rounded security professional.

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

Learn the best ways to test your own systems before the bad guys attack.

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

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

You will learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today.

After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

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

“SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective.”
-Steve Nolan, General Dynamics

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone’s renowned penetration testing team, and he served as a senior instructor and co-author of Foundstone’s *Ultimate Hacking: Hands-On* course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute’s most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who’s who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world.
All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been greater 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.

FOR500: 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 understand, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn to recover, analyze, and authenticate forensic data on Windows systems. You’ll 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. You’ll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, 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 10 artifacts.

MASTER WINDOWS FORENSICS — YOU CAN’T PROTECT WHAT YOU DON’T KNOW ABOUT

Kevin Ripa is the owner of Computer Evidence Recovery, Inc., and past president of the Alberta Association of Private Investigators. He is a former member of the Department of National Defense, where he served in both foreign and domestic postings. He currently provides services to various levels of law enforcement, Fortune 500 companies, and the legal community, and has assisted in many complex cyber-forensics and hacking response investigations around the world. Kevin has over 25 years of experience in the digital investigations field, having started doing forensics before the days of GUI response and vendor training. He is sought-after for his expertise in information technology investigations, and he has been qualified as an expert witness on numerous occasions at virtually all levels of the judicial process. He has also designed, produced, hosted, and taught numerous industry-related courses, and has had over 100 speaking and training engagements with industry and law enforcement around the world. Kevin holds a number of industry certifications, including the GCFE, GCFA, GSEC, GISF, EnCase Certified Examiner, Certified Data Recovery Professional, and Licensed Private Investigator. He has also authored dozens of articles, as well as chapters in a number of manuals, books, and training texts on computer security and forensics.

Kevin Ripa
SANS Instructor
@kevinripa

“Six-Day Program
Mon, Sep 10 - Sat, Sep 15
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Kevin Ripa

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

“Three course is a must-do for all incident responders and computer security incident response team leads to be able to answer critical questions quickly and determine the scope of an incident.”
-Brad Milhorn,
NTT Data Services
Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization’s ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools. The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen’s capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files’ structure to bypass the packer’s protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systematic manner. When performing the exercises, you will study the supplied specimens’ behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

Jake Williams is a principal consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. He is well-versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation.

Six-Day Program
Mon, Sep 10 - Sat, Sep 15
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jake Williams

Who Should Attend
- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

“The complexity of malware these days is amazing. This course has helped me to understand the tools and processes to fight back.”
- Andrew Danen, Regions Bank

Jake Williams
SANS Senior Instructor
@MalwareJake

Register at www.sans.org/baltimore-fall | 301-654-SANS (7267)
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.

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!

For course updates, prerequisites, special notes, or laptop requirements, visit: www.sans.org/event/baltimore-fall-2018/courses

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master’s degree in business administration, and a master’s degree in strategic studies, and holds the GSLC, CISSP®, CISM and CISA certifications.

G. Mark Hardy
SANS Principal Instructor
@g_mark

For course updates, prerequisites, special notes, or laptop requirements, visit: www.sans.org/event/baltimore-fall-2018/courses
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? How do we turn this into a continuous monitoring process? 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.

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.

You’ll be able to use what you learn immediately. Five of the six days in the course will help you produce your own checklist, or provide you 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 six 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.

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 gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

Six-Day Program
Mon, Sep 10 - Sat, Sep 15
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Clay Risenhoover

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
- Anyone looking to implement effective continuous monitoring processes within the enterprise

Six-Day Program
Mon, Sep 10 - Sat, Sep 15
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Clay Risenhoover

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
- Anyone looking to implement effective continuous monitoring processes within the enterprise

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? How do we turn this into a continuous monitoring process? 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.

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.

You’ll be able to use what you learn immediately. Five of the six days in the course will help you produce your own checklist, or provide you 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 six 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.

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 gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

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 past 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®.
Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization’s security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation. The use of professional services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations. A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEMs and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.

The goal of this course is to teach students how to build a SIEM from the ground up using the Elastic Stack. Throughout the course, students will learn about the required stages of log collection. We will cover endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, and we will combine these components to make a flexible, high-performance SIEM solution. Using this approach empowers SIEM engineers and analysts to understand the complete system, make the best use of technology purchases, and supplement current underperforming deployments. This process allows organizations to save money on professional services, increase the efficiency of internal labor, and develop a nimbler solution than many existing deployments. For example, many organizations pay thousands of dollars in consulting fees when a unique log source needs a custom parser. This course will train students how to easily parse any log source without requiring consulting services, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

Find a full description of this course at www.sans.org/event/baltimore-fall-2018/courses.

As the number and complexity of cybersecurity attacks continues to increase, it is more important than ever that organizations have the ability to measure risk from various scenarios and prioritize the scenarios with the largest forecasted losses for mitigation. Once a scenario is selected for mitigation, it is critical that the most cost-effective solution be chosen – that is, the solution that reduces the largest amount of risk per dollar spent in implementation. FAIR-based risk analysis enables these decisions and many more. Deriving meaningful measurements of risk in dollars requires an accurate model of risk. This course will teach you the fundamentals of the FAIR model, the international standard model for quantifying risk invented by Jack Jones and endorsed by The Open Group and many other organizations. You will master the foundational terms and definitions of quantitative risk analysis, understand the different factors of risk and how they interact, and be able to apply the FAIR model to real-life case studies to quantify risk using calibrated estimates and Monte Carlo simulation. This foundational knowledge and experience will prepare you to successfully attain the Open Group’s OpenFAIR Certification.

Find a full description of this course at www.sans.org/event/baltimore-fall-2018/courses.
Two FREE Nights of Core NetWars at SANS Baltimore Fall 2018!*

SEPTEMBER 13 & 14 6:30-9:30 PM

The Core NetWars Experience is a computer and network security challenge designed to test your experience and skills in a safe, controlled environment while you have a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you’ll build a wide variety of skills while having a great time.

Come and join us for these exciting events to test your skills in a challenging and fun learning environment.

*CORE NETWARS IS FREE OF CHARGE TO ALL STUDENTS AT SANS BALTIMORE FALL 2018.

www.sans.org/baltimore-fall
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:

**Blockchain: Building Better Business Models Securely** – G. Mark Hardy
Blockchain as a technology has been proposed as a solution to everything from frictionless currency transfer to tracking cargo on ships. With over $1 billion in venture funds invested and several hundred patents filed, every security professional must know the impact on organizations in terms of risk, volatility, and competitiveness. This talk will explain blockchain technology, how it can do much more than cryptocurrencies like Bitcoin, and the basics of “smart contracts.” We’ll separate the hype from the fact, and look at the security implications of placing corporate information in an unalterable distributed ledger. Most importantly, we’ll discuss how to identify business processes at your organization that can be improved or enabled by this technology (hint: if you just substitute blockchain for database, it’s not a good fit). Come explore the future of blockchain technology, and gain a working knowledge of how to provide a framework for utilizing and securing a technology considered as disruptive as the Internet was in the 1990s.

**OODA Security: Taking Back the Advantage** – Kevin Fiscus
OODA, or Observe, Orient, Decide and Act, is a concept first developed for fighter pilots. The concept states that the adversary who can effectively complete the OODA cycle first will go home while the adversary who takes longer enjoys, at best, a long, slow parachute ride to the ground. This concept can be applied to information security. In theory, we believe that if our “house” the attackers are attacking. Unfortunately, that is rarely the case. Over 50% of organizations find out they have been compromised via notification by a third party, meaning that all too often defenders don’t even start their OODA loop until after the attacker has completed the compromise. Making things worse, traditional security controls are failing us because attackers already know how to circumvent or evade them. Fortunately, there is a solution. By making better use of our existing technology and by using some of the attackers’ tools and techniques against them, we can deter, distract, delay, disrupt and detect attackers. Come learn how we can turn the tables on the bad guys and reclaim the OODA loop initiative.

**InfoSec State of the Union** – Jake Williams
In this presentation Jake will address current topics in cybersecurity discussing the intersection of tech, policy, and ethics. Because it’s impossible to know what will be in the news as we go to print with these abstracts, talk to Jake for an up-to-date list of what he’ll be discussing in this session. Past sessions have addressed hacking cases, data breaches, impact of nation-state malware leaks, hacking the voting system, and state-sponsored cyber espionage.

**Zero Trust Architecture** – Justin Henderson
Perimeter security and other architecture models continue to fail us. The truth is that users and systems continue to accumulate access over time, and the inside of a network tends to be wide open for the picking. Instead of designing defenses around an outdated architecture, come and learn about zero trust architecture. Zero trust allows you to stray away from the old saying of “trust but verify” and instead switch to a “verify all” approach. No budget, no worries. This presentation focuses on implementing zero trust with systems and software you already own. What can I say, blue team is awesome!

**Why The Bad Guys Win** – Kevin Ripa
How frustrating is it when another pedophile skates on a possession charge? How many times has your evidence been successfully challenged? This can make any anyone question why they should even bother. This lecture will look at the three biggest mistakes made by law enforcement and prosecutors, and at how to ensure that those mistakes are not made in the future. We will also look at two of the biggest sham defenses used in court, and how to successfully defeat them! This is a must attend for law enforcement, prosecutors, and anyone else who might end up in a court room.

**So, You Want To Be An Infosec Consultant?** – Ted Demopoulos
Becoming a successful consultant seems like a dream: high pay, freedom, and fascinating work. These can all be true yet there is more to the reality: as a consultant you are running a business and you need clients! This session covers what those considering consulting need to know, including starting the business, getting clients, pricing, and much more. Whether you aspire to consulting full time or you want to keep your job and consult on the side, we cover the basics you need to know to get started.

**Moving Past Just Googling It: Harvesting and Using OSINT** – Micah Hoffman
Every single day we search for things on the Internet. Defenders research a domain or IP that contains malware. Attackers look for email addresses for an upcoming phishing campaign. DFIR people examine locations and usernames that they acquired from a subject’s computer. Policy and compliance people examine the risk that employees in their organizations might bring to work. Recruiters scour the Internet looking for candidates. And normal people shop, date, geolocate, post, tweet, and otherwise send a huge amount of data to the public Internet. Come join Micah Hoffman as we examine how open-source intelligence can reveal interesting content about your work and personal lives.
**Future Training Events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Jun 25-30</td>
</tr>
<tr>
<td>Vancouver</td>
<td>Vancouver, BC</td>
<td>Jun 25-30</td>
</tr>
<tr>
<td>Charlotte</td>
<td>Charlotte, NC</td>
<td>Jul 9-14</td>
</tr>
</tbody>
</table>

**SANSFIRE**

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boston Summer</td>
<td>Boston, MA</td>
<td>Aug 6-11</td>
</tr>
<tr>
<td>San Antonio</td>
<td>San Antonio, TX</td>
<td>Aug 6-11</td>
</tr>
<tr>
<td>New York City Summer</td>
<td>New York, NY</td>
<td>Aug 13-18</td>
</tr>
<tr>
<td>Northern VA – Alexandria</td>
<td>Alexandria, VA</td>
<td>Aug 13-18</td>
</tr>
<tr>
<td>Virginia Beach</td>
<td>Virginia Beach, VA</td>
<td>Aug 20-31</td>
</tr>
<tr>
<td>Chicago</td>
<td>Chicago, IL</td>
<td>Aug 20-25</td>
</tr>
<tr>
<td>San Francisco Summer</td>
<td>San Francisco, CA</td>
<td>Aug 26-31</td>
</tr>
<tr>
<td>Tampa-Clearwater</td>
<td>Tampa, FL</td>
<td>Sep 4-9</td>
</tr>
<tr>
<td>Baltimore Fall</td>
<td>Baltimore, MD</td>
<td>Sep 8-15</td>
</tr>
</tbody>
</table>

**Network Security**

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Fall – Tysons</td>
<td>Tysons, VA</td>
<td>Oct 13-20</td>
</tr>
<tr>
<td>Denver</td>
<td>Denver, CO</td>
<td>Oct 15-20</td>
</tr>
<tr>
<td>Seattle Fall</td>
<td>Seattle, WA</td>
<td>Oct 15-20</td>
</tr>
<tr>
<td>Houston</td>
<td>Houston, TX</td>
<td>Oct 29 - Nov 3</td>
</tr>
<tr>
<td>Dallas Fall</td>
<td>Dallas, TX</td>
<td>Nov 5-10</td>
</tr>
<tr>
<td>San Diego Fall</td>
<td>San Diego, CA</td>
<td>Nov 12-17</td>
</tr>
<tr>
<td>Austin</td>
<td>Austin, TX</td>
<td>Nov 26 - Dec 1</td>
</tr>
<tr>
<td>San Francisco Fall</td>
<td>San Francisco, CA</td>
<td>Nov 26 - Dec 1</td>
</tr>
<tr>
<td>Nashville</td>
<td>Nashville, TN</td>
<td>Dec 3-8</td>
</tr>
</tbody>
</table>

**Future Summit Events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness</td>
<td>Charleston, SC</td>
<td>Aug 6-15</td>
</tr>
<tr>
<td>Data Breach</td>
<td>New York City, NY</td>
<td>Aug 20-27</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response</td>
<td>New Orleans, LA</td>
<td>Sep 6-13</td>
</tr>
<tr>
<td>Alaska</td>
<td>Anchorage, AK</td>
<td>Sep 10-15</td>
</tr>
<tr>
<td>Oil &amp; Gas Cybersecurity</td>
<td>Houston, TX</td>
<td>Oct 1-6</td>
</tr>
<tr>
<td>Secure DevOps</td>
<td>Denver, CO</td>
<td>Oct 22-29</td>
</tr>
<tr>
<td>Pen Test HackFest</td>
<td>Bethesda, MD</td>
<td>Nov 12-19</td>
</tr>
</tbody>
</table>

**Future Community SANS Events**

Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.
Register online at www.sans.org/baltimore-fall
We recommend you register early to ensure you get your first choice of courses.
Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Cancellation & Access Policy
If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org.
If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by August 22, 2018. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

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

Pay Early and Save*
Use code EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>Pay &amp; enter code by</th>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7-18-18</td>
<td>$400.00</td>
<td>8-8-18</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS Voucher Program
Expand your training budget!
Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.
www.sans.org/vouchers

Top 3 reasons to stay at the Hilton Baltimore
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton Baltimore, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton Baltimore that you won’t want to miss!

Special Hotel Rates Available
A special discounted rate of $212.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.
Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through August 16, 2018.

Hilton Baltimore
401 W. Pratt Street
Baltimore, MD 21201
443-573-8700
www.sans.org/event/baltimore-fall-2018/location

Hilton Baltimore is set in the Inner Harbor, an iconic seaport area of restaurants, museums, shops, sports complexes, nightclubs, and historic ships. The hotel is a quick walk to Camden Yards, M&T Stadium, the National Aquarium, Maryland Science Center, and a waterfront concert at Pier Six Pavilion.

Hotel Information
Hilton Baltimore
401 W. Pratt Street
Baltimore, MD 21201
443-573-8700
www.sans.org/event/baltimore-fall-2018/location

Top 3 reasons to stay at the Hilton Baltimore
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton Baltimore, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton Baltimore that you won’t want to miss!

Special Hotel Rates Available
A special discounted rate of $212.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.
Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through August 16, 2018.

Hotel Information
Hilton Baltimore
401 W. Pratt Street
Baltimore, MD 21201
443-573-8700
www.sans.org/event/baltimore-fall-2018/location

Hilton Baltimore is set in the Inner Harbor, an iconic seaport area of restaurants, museums, shops, sports complexes, nightclubs, and historic ships. The hotel is a quick walk to Camden Yards, M&T Stadium, the National Aquarium, Maryland Science Center, and a waterfront concert at Pier Six Pavilion.

Special Hotel Rates Available
A special discounted rate of $212.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.
Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through August 16, 2018.

Hotel Information
Hilton Baltimore
401 W. Pratt Street
Baltimore, MD 21201
443-573-8700
www.sans.org/event/baltimore-fall-2018/location

Hilton Baltimore is set in the Inner Harbor, an iconic seaport area of restaurants, museums, shops, sports complexes, nightclubs, and historic ships. The hotel is a quick walk to Camden Yards, M&T Stadium, the National Aquarium, Maryland Science Center, and a waterfront concert at Pier Six Pavilion.

Special Hotel Rates Available
A special discounted rate of $212.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.
Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through August 16, 2018.
Join the SANS.org community today to enjoy these free resources at www.sans.org/account

Newsletters

NewsBites
Twice-weekly, high-level executive summaries 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.

Webcasts

Ask the Experts 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 how a vendor’s commercial tool can be used to solve or mitigate that problem.

Other Free Resources (No SANS account is necessary)

- 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)

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by June 13th. www.sans.org/boston-summer

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.