THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

# SANS Baltimore 2013

Baltimore, MD | October 14-19

*The Most Intense Information Security Training in Maryland*

*Featuring these popular courses:*

- Security Essentials Bootcamp Style
- Hacker Techniques, Exploits, and Incident Handling
- Intrusion Detection In-Depth
- Security Leadership Essentials For Managers with Knowledge Compression™
- SANS +S Training Program for the CISSP® Certification Exam
- Advanced Computer Forensic Analysis and Incident Response
- Implementing and Auditing the Twenty Critical Security Controls – In-Depth

*Our **NEW!** Audit courses:*

- Auditing Security and Controls of Active Directory and Windows
- Auditing Security and Controls of Oracle Databases

*"Cutting-edge expertise taught by world-class experts."*

-Joseph Murray, Deloitte

GIAC Approved Training

**Register at www.sans.org/event/baltimore-2013**

**Save $500** by registering early!

See page 13 for more details.

Dear Colleague,

We are pleased to invite you to **SANS Baltimore 2013** from **October 14-19**. This is a full SANS training event along with *SANS@Night* evenings, which will enhance your training, all included in your tuition.

Our instructor team includes many of SANS most requested faculty: Dr. Eric Cole, Hal Pomeranz, James Tarala, Dr. Johannes Ulrich, Tanya Baccam wrote and teach many of our most popular courses along with G. Mark Hardy, Seth Misenar, Peter Szczepankiewicz, and Bryan Simon. This team will ensure that you not only learn the material but that you will be able to use what you have mastered the day you get back to your office.

SANS Baltimore 2013 offers you a chance to take both of our two new three-day audit courses: A*UD444: Auditing Security and Controls of Active Directory and Windows* and *AUD445: Auditing Security and Controls of Oracle Databases*. Choose one of our most-taken security courses, our advanced forensics course, or one of two security management courses. SANS Baltimore 2013 features this variety of courses chosen to boost your career. Please use this brochure to view our comprehensive course descriptions, our instructor bios, our evening events and talks that add to what you learn. We think you will find this event interesting and inviting.

Six of our courses will prepare you or your technical staff for *DoD Directive 8570* and *GIAC* approved certification exams along with counting toward your *STI Master's Degree*.

SANS Baltimore 2013 takes place at the **Baltimore Marriott Inner Harbor at Camden Yards** in the downtown Inner Harbor district. It is close to Oriole Park at Camden Yards and the Ravens' Stadium. A special discounted rate of $199 S/D will be honored based on space availability. This special rate is only available until September 23, 2013. Government per diem rooms are available with proper ID. You must call the hotel and specifically ask for this rate. These rates will include high-speed Internet in your room.

Now more than ever, this hands-on, immersion information security training experience will set you apart from others in the field. So, register today for SANS Baltimore 2013 and get the best computer security training money can buy.

Please feel free to drop me a note (**ebassel@sans.org**) if I can answer any of your questions about meeting the Department of Defense Directive 8570.

*Eric Bassel*
Eric Bassel
SANS Director

**Eric Bassel**

Here's what SANS alumni have said about the value of SANS training:

*"SANS is always professional organized, flexible, friendly, and personable. I will definitely do busines again with you and recommend you to peers."*
-Sarah McVey,
Lane County Government

*"This was an awesome and informative experience. My organization will benefit as a result. Thanks!"*
-Far'd Thomas,
Lockheed Martin

*"The class is exceeding my expectations, which were already very high. I am very happy with the class and instructor."*
-David Mashburn,
US Pharmacopeia

## Courses-at-a-Glance

| | | MON 10/14 | TUE 10/15 | WED 10/16 | THU 10/17 | FRI 10/18 | SAT 10/19 |
|---|---|---|---|---|---|---|---|
| SEC401 | Security Essentials Bootcamp Style | PAGE 1 | | | | | |
| SEC503 | Intrusion Detection In-Depth | PAGE 2 | | | | | |
| SEC504 | Hacker Techniques, Exploits, and Incident Handling | PAGE 3 | | | | | |
| SEC566 | Implementing and Auditing the Twenty Critical Security Controls – In-Depth | PAGE 4 | | | | | |
| FOR508 | Advanced Computer Forensic Analysis & Incident Response | PAGE 5 | | | | | |
| MGT414 | SANS +S Training Program for the CISSP® Cert Exam | PAGE 6 | | | | | |
| MGT512 | SANS Security Leadership Essentials For Managers with Knowledge Compression™ | PAGE 7 | | | | | |
| AUD444 | Auditing Security and Controls of Active Directory and Windows | | | | PAGE 8 | | |
| AUD445 | Auditing Security and Controls of Oracle Databases | PAGE 8 | | | | | |

SECURITY 401

# Security Essentials Bootcamp Style

**Six-Day Program • Mon, Oct 14 – Sat, Oct 19**
**9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)**
**46 CPE/CMU Credits • Laptop Required**
**Instructor: Seth Misenar**

It seems wherever you turn organizations are being broken into and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore we will teach you how to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure.

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

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While 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 works in cyber security. 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 cyber security, three questions must be answered:

1. **What is the risk?**
2. **Is it the highest priority risk?**
3. **Is it the most cost-effective way of reducing the risk?**

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared 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 gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.**


**www.giac.org**


**www.sans.edu**


**www.sans.org/cyber-guardian**

DoDD 8570 Required
**www.sans.org/8570**

## Seth Misenar *SANS Certified Instructor*

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including SEC401: SANS Security Essentials Bootcamp Style, SEC504: Hacker Techniques, Exploits, and Incident Handling, and SEC542: Web App Penetration Testing and Ethical Hacking. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute.

SECURITY 503

# Intrusion Detection In-Depth

**Six-Day Program • Mon, Oct 14 – Sat, Oct 19**
**9:00am - 5:00pm • 36 CPE/CMU Credits**
**Laptop Required • Instructor: Dr. Johannes Ullrich**

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

## Who Should Attend:

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

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

*"Johannes's excellent knowledge in application protocols has enabled us to get an in-depth understanding of them."*
-Karthik K., Symantec

*"This course is valuable for anyone interested in IDS. The instructor's knowledge and willingness to help you understand the material are unlike any other training I've been to. Great course and instructor."*
-Dannie Arnold, U.S. Army

Hands-on exercises supplement the coursebook material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches – a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material to have a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.


www.giac.org


www.sans.edu


www.sans.org/cyber-guardian

DoDD 8570 Required
www.sans.org/8570

## Dr. Johannes Ullrich *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. Prior to working for SANS, Johannes worked as a lead support engineer for a Web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also maintains a daily security news summary podcast (**http://isc.sans.edu/podcast.html**) and enjoys blogging about application security. **http://software-security.sans.org/blog**

Simulcast *Attend Remotely Via Simulcast*
**www.sans.org/event/baltimore-2013/attend-remotely**

SECURITY 504

# Hacker Techniques, Exploits, and Incident Handling

**Six-Day Program • Mon, Oct 14 – Sat, Oct 19**
**9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)**
**Laptop Required • 37 CPE/CMU Credits**
**Instructor: Peter Szczepankiewicz**

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well-suited to individuals who lead or are a part of an incident handling team. Furthermore, 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.

*"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."*
-Joshua Anthony, West Virginia Army National Guard

## Who Should Attend:

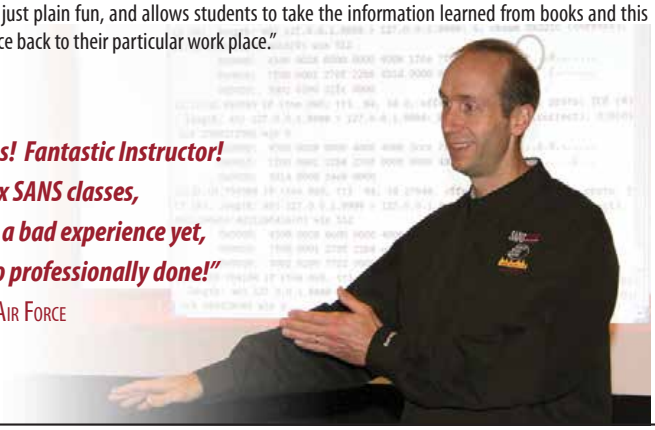
- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.

*"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."*
-Anthony Liu, Scotia Bank

## Peter Szczepankiewicz *SANS Certified Instructor*

Formerly working with the military, Peter responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a senior security engineer with IBM. People lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. Peter expounds, "Putting together networks only to tear them apart, is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place."



*"Fantastic class! Fantastic Instructor! I have taken six SANS classes, I have not had a bad experience yet, they are just so professionally done!"*
-Rafael Cabrera, Air Force

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

DoDD 8570 Required
www.sans.org/8570

SECURITY 566

# Implementing and Auditing the Twenty Critical Security Controls – In-Depth

**Five-Day Program • Mon, Oct 14 – Fri, Oct 18**
**9:00am - 5:00pm • 30 CPE/CMU Credits**
**Laptop Required • Instructor: James Tarala**

## 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

**SPECIAL NOTE:** This in-depth course has been updated to incorporate new attack vectors published in version 4.0 of Critical Controls released November 5, 2012. **www.sans.org/critical-security-controls**

Cybersecurity attacks are increasing and evolving so rapidly that 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 Twenty 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.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.

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 organization in order to improve its cyber defense."

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 though 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.

## James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

Simulcast *Attend Remotely Via Simulcast*
**www.sans.org/event/baltimore-2013/attend-remotely**

FORENSICS 508

# Advanced Computer Forensic Analysis and Incident Response

**Six-Day Program • Mon, Oct 14 – Sat, Oct 19**
**9:00am - 5:00pm • 36 CPE/CMU Credits**
**Laptop Required • Instructor: Hal Pomeranz**

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

***DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.***

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

***FOR508: Advanced Computer Forensic Analysis and Incident Response*** will help you determine:

- **How did the breach occur?**
- **What systems were compromised?**
- **What did they take? What did they change?**
- **How do we remediate the incident?**

The updated FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

***"Excellent course, invaluable hands-on experience taught by people who not only know the tools and techniques, but know their quirkiness through practical, real-world experience."***
-John Alexander, US Army

***"Absolutely essential knowledge. Traditional knowledge is useful, but this course provides the practical side of a growing trend.***
-Erik Musick, Arkansas State Police

## Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is the founder and technical lead for Deer Run Associates, a consulting company focusing on Digital Forensics and Information Security. He is a SANS Faculty Fellow and the creator of the SANS/GIAC Linux/Unix Security course (GCUX), as well as being an instructor in the SANS Forensics curriculum. An expert in the analysis of Linux and Unix systems, Hal provides forensic analysis services through his own consulting firm and by special arrangement with MANDIANT. He has consulted on several major cases for both law enforcement and commercial clients. Hal is a regular contributor to the SANS Computer Forensics blog (**http://computer-forensics.sans.org/blog**), and co-author of the weekly Command-Line Kung Fu blog (**http://blog.commandlinekungfu.com**).

## Who Should Attend:

- **Information security professionals**
- **Incident response team members**
- **Experienced digital forensic analysts**
- **Federal agents and law enforcement**
- **Red team members, penetration testers, and exploit developers**
- **SANS FOR408 and SEC504 graduates**

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.**

DFIR
**http://computer-forensics.sans.org**

**www.giac.org**

**www.sans.edu**

**www.sans.org/cyber-guardian**

DoDD 8570 Required
**www.sans.org/8570**

MANAGEMENT 414

# SANS® +S™ Training Program for the CISSP® Certification Exam

**Six-Day Program • Mon, Oct 14 – Sat, Oct 19**
**9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)**
**8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits**
**Laptop NOT Required • Instructor: Dr. Eric Cole**

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

**Domain 1: Access Controls**
**Domain 2: Telecommunications and Network Security**
**Domain 3: Information Security Governance & Risk Management**
**Domain 4: Software Development Security**
**Domain 5: Cryptography**
**Domain 6: Security Architecture and Design**
**Domain 7: Security Operations**
**Domain 8: Business Continuity and Disaster Recovery Planning**
**Domain 9: Legal, Regulations, Investigations and Compliance**
**Domain 10: Physical (Environmental) Security**

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

## Obtaining your CISSP® certification consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of résumé**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Period Audit of CPEs to maintain the credential**

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

*"This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent."*
-Jeff Jones, Constellation Energy Group

*"This class focuses like a laser on the key concepts you'll need to understand the CISSP exam. Don't struggle with thousand page textbooks – let this course be your guide!"*
-Carl Williams, Harris Corporation

## 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® 10 Domains**
- **Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job**

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

## Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including ***Advanced Persistent Threat***, ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible*** 2nd Edition, and ***Insider Threat***. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.**

**www.giac.org**

DoDD 8570 Required
**www.sans.org/8570**

**Simulcast** *Attend Remotely Via Simulcast*
**www.sans.org/event/baltimore-2013/attend-remotely**

MANAGEMENT 512

# SANS Security Leadership Essentials For Managers with Knowledge Compression™

**Five-Day Program • Mon, Oct 14 – Fri, Oct 18**
**9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)**
**33 CPE/CMU Credits • Laptop NOT Required • Instructor: G. Mark Hardy**

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will gain 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.

## 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 your technical people are telling you

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.

*"Tremendously valuable experience!! Learned a lot and also validated a lot of our current pratices. Thank you!!"*
-Chad Gray, Booz Allen Hamilton

*"Every IT security professional should attend no matter what their position. This information is important to everyone."*
-John Flood, NASA

## G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM, and CISA certifications.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.**

www.giac.org

www.sans.edu

DoDD 8570 Required
www.sans.org/8570

Simulcast *Attend Remotely Via Simulcast*
www.sans.org/event/baltimore-2013/attend-remotely

AUDIT 444

## Auditing Security and Controls of Active Directory and Windows

NEW!

**Three-Day Program • Thu, Sept 17 - Sat, Sept 19**
**9:00am - 5:00pm • 18 CPE/CMU Credits**
**Laptop Required | Instructor: Bryan Simon**

### Who Should Attend:

- Internal auditors
- IT specialist auditors
- IT auditors
- IT audit managers
- Information system auditors
- Information security officers

Auditors need to be able to understand how Active Directory operates and the key business risks that are present. This course was written to teach auditors how to identify and assess those business risks. Active Directory and Windows systems are typically well known and utilized within organizational infrastructures. However, they can be difficult to audit since there are a large number of settings on the end system. This course provides the tools and techniques to effectively conduct an Active Directory and Windows audit, and while doing so identify key business process controls that may be missing. Students have the opportunity to look at the business process controls and then how those can be verified by looking at Active Directory and the Windows systems that exist. Plus, students are given the knowledge to be able to add additional value as part of their audits by being able to identify the technology risks that may have been overlooked. The hands-on exercises reinforce the topics discussed in order to give students the opportunity to conduct an audit on their own Windows systems, as well as understand the different security options that Windows provides.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.**

AUDIT 445

## Auditing Security and Controls of Oracle Databases

NEW!

**Three-Day Program • Mon, Sept 14 - Wed, Sept 16**
**9:00am - 5:00pm • 18 CPE/CMU Credits**
**Laptop Required | Instructor: Bryan Simon & Tanya Baccam**

### Who Should Attend:

- Internal auditors
- IT specialist auditors
- IT auditors
- IT audit managers
- Information system auditors
- Information security officers

Over the past few years we have seen attackers target data, since there is a financial incentive to being able to compromise valuable data. The media seem to be reporting new data compromises constantly. That means auditors need to be effectively auditing the controls that should exist to protect this valuable organizational asset.

Oracle Databases often store the data that's being targeted. Oracle Databases are very complex and challenging to audit! Auditors need to be able to effectively audit the processes and controls in place around the database to ensure the asset is being properly protected and the risks properly managed.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/baltimore-2013.**

This course provides all of the details, including the IT process, and procedural and technical controls that you as an auditor should look for when conducting an Oracle database audit. Even better, you have the opportunity to get firsthand experience extracting and interpreting data from a live Oracle Database, which allows you to be able to return and immediately conduct an Oracle Database audit. By getting hands-on experience, you get a better understanding of exactly how an Oracle Database operates and what data is available for audit purposes. The course is also put together in such a way that you can add additional value to the business and provide further security recommendations and benefits for the database being audited.

***"This course is full of relevant, timely, current content, delivered in a highly engaging style. This course is a must for IT auditors and security specialists."***

-Brooks Adams,
Georgia Southern University

# Bonus Sessions

## SANS@Night Evening Talks

***Enrich your SANS training experience! Evening talks given 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: APT: It is Time to Act *Dr. Eric Cole*

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

### An Introduction to PowerShell for Security Assessments *James Tarala*

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone "all in" with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of the Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

### The Security Impact of IPv6 *Dr. Johannes Ullrich*

IPv6 is more then just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the "DC" to "AC" conversion in the electric world. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocols opportunities are not well understood, and IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody's pet.

### Hacking as an Act of War *G. Mark Hardy*

Once the exclusive domain of a small number of highly intelligent introverts, hacking has gone "mainstream" as an element of national defense. The United States has established a four-star Cyber Command to provide coordinated military digital response after suffering massive data breaches. NATO established the Cooperative Cyber Defence Center of Excellence in Estonia after that nation was the target of extensive cyber attacks. At what point does hacking (read, "computer network attack") rise to the level of warfare? What role should we play as cyber-citizens?

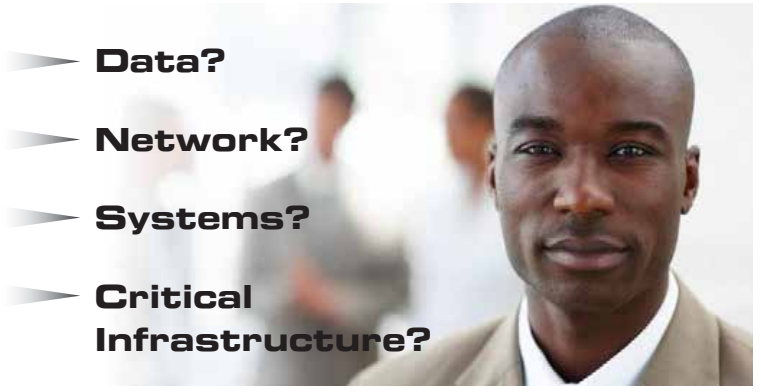
### Introducing the CompTIA® CASP™ Exam *Seth Misenar*

Seth Misenar, coauthor of *Syngress CISSP® Study Guide* (written with Eric Conrad), will introduce you to the new CompTIA® Advanced Security Practitioner certification, a hands-on technical exam with a mix of deeper technical questions, as well as higher-level management questions. The CASP™ was recently added to DoD 8570 for the following roles: IAT level III, IAM II, and IASAE level I and II. Will this cert be a valuable addition to your resume? Will this cert bleed significant market share from the CISSP? Now that it has been added to DoD8570, will CASP become the go to DoD cert? Come find out where CASP fits into the security certification landscape and see if Eric and Seth's new SANS prep course for the CASP is right for you.

### Tales from the Crypt: TrueCrypt Analysis *Hal Pomeranz*

What if you suspect a device you are investigating may contain TrueCrypt volumes? What if you have no passwords or memory image to analyze and cannot access the volumes? Is all hope lost? Based on real-world investigations, this talk starts by covering techniques for detecting TrueCrypt volumes on Windows systems using a combination of specialized tools, registry forensics, and application-specific configuration files. Next we'll look at the information that is available to the investigator about the contents of a TrueCrypt volume, even when the volume itself cannot be decrypted.

# How Are You Protecting Your




Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification.

**Get GIAC certified!**

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

*"GIAC is the only certification that proves you have hands-on technical skills."*
-Christina Ford, Department of Commerce

*"GIAC Certification demonstrates an applied knowledge versus studying a book."*
-Alan C, USMC

Global Information Assurance Certification
GIAC
www.giac.org

*Get Certified* at
**www.giac.org**

## Department of Defense Directive 8570
### *(DoDD 8570)*
www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

## SANS Training Courses for DoDD Approved Certifications

| SANS TRAINING COURSE | | DoDD APPROVED CERT |
|---|---|---|
| SEC401 | Security Essentials Bootcamp Style | GSEC |
| SEC501 | Advanced Security Essentials - Enterprise Defender | GCED |
| SEC503 | Intrusion Detection In-Depth | GCIA |
| SEC504 | Hacker Techniques, Exploits & Incident Handling | GCIH |
| AUD507 | Auditing Networks, Perimeters, and Systems | GSNA |
| FOR508 | Advanced Computer Forensic Analysis and Incident Response | GCFA |
| MGT414 | SANS® +S™ Training Program for the CISSP® Certification Exam | CISSP |
| MGT512 | SANS Security Essentials for Managers with Knowledge Compression™ | GSLC |

### Compliance/Recertification:

To stay compliant with DoD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

***DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.***

***For more information, contact us at 8570@sans.org or visit www.sans.org/8570***


**WASHINGTON, DC** | **SUMMIT: NOV 7-8** | **COURSES: NOV 9-14**

**COURSES AVAILABLE: SEC560 | SEC575 | SEC642 | SEC660**

SANS is hosting our ultimate annual penetration testing training event in November. Featuring top-notch talks, in-depth training, and evening activities to help participants build awesome skills, the SANS Pen Test Hackfest Summit and Training Event is specially designed for penetration testers across a broad range of skills and disciplines. Here are the top 5 reasons to attend this event:


**NetWars!** 4 full-evenings of hands-on challenges


**CyberCity!** Participate in SANS first-ever hands-on CyberCity missions at a training event

**Coin-a-Palooza!** Earn up to 4 SANS PenTest CtF coins during evening challenges

**Expert Speakers** on cutting-edge attack and defense topics

**Top-Notch Courses,** including: **SEC560 | SEC575 | SEC642 | SEC660**

*Learn more at* **www.sans.org/event/pen-test-hack-fest-2013**

# SECURITY AWARENESS
## FOR THE 21st CENTURY


- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPPA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org

# What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

***The SANS Technology Institute (STI) offers two unique master's degree programs:***

**Master of Science in Information Security Engineering**

**Master of Science in Information Security Management**

*"A degree is great. A graduate degree plus current actionable knowledge is even better. STI provides this and more."*
-Seth Misenar, MSISE Student

***Apply today!***
***Cohorts are forming now.***


www.sans.edu
info@sans.edu
720.941.4932

## Future SANS Training Events

***Get complete information on all future training events at www.sans.org/security-training/by-location/all***

SANS **Virginia Beach** 2013
Virginia Beach, VA | Aug 19-30

SANS **Capital City** 2013
Washington, DC | Sept 3-8

**Network Security** 2013
Las Vegas, NV | Sept 14-23

SANS **Seattle** 2013
Seattle, WA | Oct 7-14

SANS **Chicago** 2013
Chicago, IL | Oct 28 - Nov 2

SANS **South Florida** 2013
Fort Lauderdale, FL | Nov 4-9

SANS **Pen Test Hackfest**
Training Event and Summit
Washington, DC | Nov 7-14

SANS **San Diego** 2013
San Diego, CA | Nov 18-23

SANS **San Antonio** 2013
San Antonio, TX | Dec 3-8

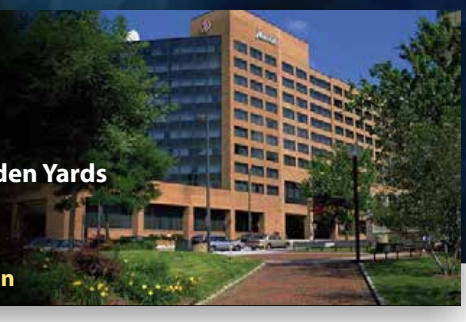
SANS **CDI** 2013
Washington, DC | Dec 12-17

SANS **Golden Gate** 2013
San Francisco, CA | Dec 16-21

SANS **Security East** 2014
New Orleans, LA | Jan 18-27

SANS Baltimore 2013

# Hotel Information



*Training Campus*
**Baltimore Marriott Inner Harbor at Camden Yards**

**110 S. Eutaw Street**
**Baltimore, MD 21210-1608**
**www.sans.org/event/baltimore-2013/location**

## Special Hotel Rates Available

**A special discounted rate of $199.00 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 September 23, 2013. To make reservations please call (800) 228-9290 and ask for the SANS group rate.**

The Baltimore Marriott Inner Harbor Hotel at Camden Yards is centrally located in the heart of Baltimore, Maryland. Sports enthusiasts will enjoy our Inner Harbor hotel's close proximity to Oriole Park at Camden Yards and the Ravens' M&T Bank Stadium. The spacious guest rooms, delicious onsite restaurants & state-of-the-art fitness center make the hotel a leader among Baltimore Inner Harbor hotels in style & service.

## Top 5 reasons to stay at the Baltimore Marriott Inner Harbor

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Baltimore Marriott, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Baltimore Marriott that you won't want to miss!
5. Everything is in one convenient location!

SANS Baltimore 2013

# Registration Information


*We recommend you register early to ensure you get your first choice of courses.*
**Register online at www.sans.org/event/baltimore-2013**

## To register, go to
**www.sans.org/event/baltimore-2013**

Select your course or courses and indicate whether you plan to test for GIAC certification.

***How to tell if there is room available in a course:***
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.

## Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at 301-654-7267 9am - 8pm ET.

## 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 September 18, 2013 – processing fees may apply.

**To register for a SANS Baltimore 2013 Simulcast course, please visit www.sans.org/event/baltimore-2013/attend-remotely**

## Register Early and Save

| | DATE | DISCOUNT | DATE | DISCOUNT |
|---|---|---|---|---|
| Register & pay by | 8/28/13 | $500.00 | 9/11/13 | $250.00 |

Some restrictions apply.

## Group Savings (Applies to tuition only)

**15% discount** if 12 or more people from the same organization register at the same time
**10% discount** if 8 - 11 people from the same organization register at the same time
**5% discount** if 4 - 7 people from the same organization register at the same time

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

## SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
**www.sans.org/vouchers**