

SANS

Anaheim 2016

Anaheim, CA

February 22-27

Eight courses to choose from:

Active Defense, Offensive Countermeasures, and Cyber Deception *NEW!*

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Intrusion Detection In-Depth

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Advanced Digital Forensics and Incident Response

Intro to Information Security

Mac Forensic Analysis

“SANS is the most comprehensive single resource for security training available.”

-BRYAN WELCH, ARRIS GROUP INC.



GIAC Approved Training

SAVE \$400 on SANS Anaheim courses!

Register and pay by Dec 30th – sans.org/anaheim-2016

SANS Instructors

SANS Instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to become SANS instructors. This guarantees what you learn in class will be up-to-date and relevant to your job. The SANS Anaheim 2016 line-up of instructors includes:



Christopher Crowley
Certified Instructor



Adrien de Beaupre
Certified Instructor



Mick Douglas
SANS Instructor



Sarah Edwards
Certified Instructor



G. Mark Hardy
Certified Instructor



Paul A. Henry
Senior Instructor



David R. Miller
SANS Instructor



Chad Tilbury
Senior Instructor

Evening Bonus Sessions

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

- **KEYNOTE: Tales from the Battlefield: Lessons in Incident Response** – Chad Tilbury
- **Evolving Threats** – Paul A. Henry
- **Overview of the New 2015 CISSP® Exam** – David R. Miller
- **Card Fraud 101** – G. Mark Hardy
- **Powercat Has Power!** – Mick Douglas
- **Complete App Pwnage with Multi-POST XSRF** – Adrien de Beaupre
- **SANS 8 Mobile Device Security Steps** – Christopher Crowley

Be sure to register and pay by Dec 30th for a \$400 tuition discount!

Courses-at-a-Glance

	MON 2-22	TUE 2-23	WED 2-24	THU 2-25	FRI 2-26	SAT 2-27
SEC301 Intro to Information Security	Page 1		SIMULCAST*			
SEC401 Security Essentials Bootcamp Style	Page 2		SIMULCAST*			
SEC503 Intrusion Detection In-Depth	Page 3		SIMULCAST*			
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4		SIMULCAST*			
SEC550 Active Defense, Offensive Countermeasures & Cyber Deception	Page 5					
FOR508 Advanced Digital Forensics and Incident Response	Page 6		SIMULCAST*			
FOR518 Mac Forensic Analysis	Page 7					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 8					

*Can't travel? Note the courses available via remote Simulcast.

Register today for SANS Anaheim 2016!
sans.org/anaheim-2016



@SANSInstitute
Join the conversation:
#SANSAnaheim

SEC301:

Intro to Information Security

Five-Day Program

Mon, Feb 22 - Fri, Feb 26

9:00am - 5:00pm

30 CPEs

Laptop Required

Instructor: David R. Miller

▶ GIAC Cert: GISF

▶ OnDemand Bundle



"The material presented in SEC301 was very insightful and filled with wonderful information."

-DANTE LEGGETTE, MECU

"SEC301 gave me a much broader understanding of security threats, terminology, processes and help resources."

-JOHN WYATT, KOHLER CO.



David R. Miller SANS Instructor

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on the topics of information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including policy writing, network architecture design to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures (PKI), security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He performs as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, Security Information and Event Management (SIEM) systems, Intrusion Detection and Protection Systems (IDS / IPS), 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, a lecturer, and a technical editor of books, curriculum, certification exams, and computer-based training videos.

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

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

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

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

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



giac.org

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

SEC401:

Security Essentials Bootcamp Style

Six-Day Program

Mon, Feb 22 - Sat, Feb 27

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

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

Laptop Required

46 CPEs

Instructor: Paul A. Henry

▶ GIAC Cert: GSEC

▶ STI Master's Program

▶ Cyber Guardian

▶ DoDD 8570

▶ OnDemand Bundle



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



Paul A. Henry SANS Senior Instructor

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

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Learn to build a security roadmap that can scale today and into the future.

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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



giac.org



sans.edu



sans.org/
cyber-guardian



sans.org/8570

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

SEC503:

Intrusion Detection In-Depth

Six-Day Program

Mon, Feb 22 - Sat, Feb 27

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Adrien de Beaupre

▶ GIAC Cert: GCIA

▶ STI Master's Program

▶ Cyber Guardian

▶ DoDD 8570

▶ OnDemand Bundle

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

Who Should Attend

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

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

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

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



“SEC503 provides real-world content and perspectives, data, and tools. The instructor is very knowledgeable and is a great educator.”

-GEORGE DIOLAMOU,

JACOB'S ENGINEERING

“SEC503 covers the best processes for intrusion analysis and how to cut out most of the network noise and identify the important traffic.”

-MIKE BOYA, WARNER BROS.



Adrien de Beaupre SANS Certified Instructor

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



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8570

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program

Mon, Feb 22 - Sat, Feb 27

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor:

Christopher Crowley

▶ GIAC Cert: GCIH

▶ STI Master's Program

▶ Cyber Guardian

▶ DoDD 8570

▶ OnDemand Bundle



“SEC504 gets you into the attacker’s mindset and thinking like the attacker, which means you know what to defend from.”

-CAMERON POLLOCK, IBM

“SEC504 is awesome!

Everything included in this course is very useful in my job as a security professional!”

-VERELEO BATEO,

KCG HOLDINGS, INC.



Christopher Crowley SANS Certified Instructor

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis.

Chris is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor-of-the-Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

The Internet is full of powerful hacking tools and bad guys using them extensively.

If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

As defenders, it is essential we understand these hacking tools and techniques.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the “oldie-but-goodie” attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

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.

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



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8570

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

SEC550:

Active Defense, Offensive Countermeasures & Cyber Deception

Five-Day Program

Mon, Feb 22 - Fri, Feb 26

9:00am - 5:00pm

30 CPEs

Laptop Required

Instructor: Mick Douglas

NEW

SANS

Who Should Attend

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

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

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

You Will Be Able To

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

What You Will Receive

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

“Great instructor with the ability to tie real-world threats to theory and practice.”

-BRUCE HENKEL, HARRIS CORP.

“Mick's excellent real-world examples and cool anecdotes broke up the course nicely. This guy rocks!”

-AARON KILBEY,
CITY OF PORTLAND



Mick Douglas SANS Instructor

Even when his job title has indicated otherwise, Mick Douglas has been doing information security work for more than 10 years. He received a bachelor's degree in communications from Ohio State University and holds the CISSP, GCIH, GPEN, GCUX, GWEB, and GSNA certifications. He currently works at Binary Defense Systems as the DFIR Practice Lead. He is always excited for the opportunity to share with others so they do not have to learn the hard way! Please join in; security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he's not “geeking out” you'll likely find him indulging in one of his numerous hobbies; photography, scuba diving, or hanging around in the great outdoors.

FOR508:

Advanced Digital Forensics and Incident Response

Six-Day Program

Mon, Feb 22 - Sat, Feb 27

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Chad Tilbury

▶ GIAC Cert: GCFA

▶ Cyber Guardian

▶ STI Master's Program

▶ DoDD 8570

▶ OnDemand Bundle



“Amazing techniques that can be used instantly in the real world. Chad is awesome!”

-JONATHAN REITNAUER, VANGUARD

“Wow! What a course, and one of the best I have attended in my learning career.”

-SRINATH KANNAN, ACCENTURE



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

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

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

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

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

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

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

Who Should Attend

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



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8570

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

Chad Tilbury SANS Senior Instructor

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the U.S. Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

FOR518:

Mac Forensic Analysis

Six-Day Program

Mon, Feb 22 - Sat, Feb 27

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Sarah Edwards

▶ OnDemand Bundle



“Sarah is an incredible instructor – her knowledge far surpasses anything I’ve ever experienced plus the reference material is invaluable.”

-BEN KECK, CIENA

“Very comprehensive in-depth coverage of the course topic. Excellent reference materials as a take-away.”

-JENNIFER B.,

INDIANA STATE POLICE



Sarah Edwards SANS Certified Instructor

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal cases, and counter-intelligence, counter-narcotic, and counter-terrorism investigations. Sarah’s research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidessNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master’s in Information Assurance from Capitol College. @iamevltwin

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice?

The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518:**

Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

Who Should Attend

- ▶ Experienced digital forensic analysts
- ▶ Law enforcement officers, federal agents, and detectives
- ▶ Media exploitation analysts
- ▶ Incident response team members
- ▶ Information security professionals
- ▶ SANS FOR408, FOR508, FOR526, FOR610, and FOR585 alumni looking to round out their forensic skills

FORENSICATE DIFFERENTLY!

FOR518: Mac Forensic Analysis will teach you:

- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- **User Activity:** How to understand and profile users through their data files and preference configurations.
- **Advanced Analysis and Correlation:** How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- **Mac Technologies:** How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

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

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program

Mon, Feb 22 - Fri, Feb 26

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

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

33 CPEs

Laptop NOT Needed

Instructor: G. Mark Hardy

▶ GIAC Cert: GSLC

▶ STI Master's Program

▶ DoDD 8570

▶ OnDemand Bundle

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!

Who Should Attend

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

"This was a great course! I feel all management should take it because it helps managers understand not only security but also technical and business concepts and issues."

-DAVID STEWART, ADM

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

-PAM L., NATIONAL NUCLEAR

SECURITY ADMINISTRATION



giac.org



sans.edu



sans.org/8570

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



G. Mark Hardy SANS Certified Instructor

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

BONUS SESSIONS – EVENING TALKS

Enrich your SANS training experience!

Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: Tales from the Battlefield: Lessons in Incident Response *Chad Tilbury*

As more organizations face off against advanced adversaries, classic incident response processes are being adapted and updated to address new threats and speed up the recovery process. “Tales from the Battlefield” will illustrate multiple real-world case studies demonstrating some exciting new approaches to incident response. Learn how incident response teams are detecting, responding, and attributing attacks from targeted attackers and get a taste for the future of incident response.

Evolving Threats *Paul A. Henry*

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

Complete App Pwnage with Multi-POST XSRF *Adrien de Beaupre*

This talk will discuss the risk posed by Cross Site Request Forgery (CSRF or XSRF) which is also known as session riding, or transaction injection. Many applications are vulnerable to XSRF, mitigation is difficult as it often requires re-engineering the entire application, and the threat they pose is often misunderstood. A live demo of identifying the vulnerability, and exploiting it by performing multiple unauthorized transactions in a single POST will be demonstrated.

Overview of the New 2015 CISSP® Exam *David R. Miller*

Are you interested in the CISSP certification? How might it improve your career? Or your business card or résumé? Or prospects for getting a new job or a pay raise at your current one? Or developing your career and moving up the ladder? Or in further developing the professional skill set you already have? This talk will look at how management views this well sought-after certification. Have you been studying for it? Do you plan to take the exam soon? On January 15, 2015, ISC², the certifying body for the CISSP certification exam, released a new set of exam objectives for the CISSP certification exam. These changes were implemented on the CISSP certification exam beginning April 15, 2015. This new set of exam objectives is a major change from the previous version of the CISSP exam. ISC² has moved and merged content to form 8 Domains of the Common Body of Knowledge, down from 10 Domains in the previous exam. It has also added numerous new topics to the objectives. You will need to know about the new material you will be tested on. Let’s talk about the new shape and topics of the 2015 CISSP Certification exam.

Card Fraud 101 *G. Mark Hardy*

Ever get a call from your bank saying your credit card was stolen, but it was still in your wallet? What’s going on here? Card fraud costs \$16 billion annually, and it’s not getting better. Target, PF Changs, Michaels, Home Depot, who’s next? Find out how these big card heists are pulled off, why chip-and-pin won’t solve the fraud problem, and how crooks compromised Apple Pay. See if your bank even bothers to use the security protections it could – we’ll have a mag stripe card reader so you can really see what’s in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

Powercat Has Power! *Mick Douglas*

An overview of powercat, what it does and why it’s built the way it is. Demos of various modes of operation will be shown! Come see chat, file transfer, and of course everyone’s favorite, relays!

SANS 8 Mobile Device Security Steps *Christopher Crowley*

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Christopher Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

Build Your Best Career

WITH!

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days
of this event for just \$659 each.

SPECIAL
PRICING



OnDemand Bundle

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

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

-ROBERT JONES, TEAM JONES, INC.



GIAC Certification

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

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

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

MORE INFORMATION

sans.org/ondemand/bundles

giac.org



Security Awareness Training by the Most Trusted Source

Computer-based Training for your Employees

- End User**
 - Phishing**
 - CIP v5**
 - ICS Engineers**
 - Developers**
 - Healthcare**
- Let employees train on their own schedule
 - Tailor modules to address specific audiences
 - Courses translated into many languages
 - Test learner comprehension through module quizzes
 - Track training completion for compliance reporting purposes
 - Test employee behavior through phishing emails



Visit SANS Securing The Human at securingthehuman.sans.org

Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand

SANS
Technology
Institute

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive and rigorous graduate education experience.

Master's Degree Programs:

- ▶ M.S. in Information Security Engineering
- ▶ M.S. in Information Security Management

Specialized Graduate Certificates:

- ▶ Cybersecurity Engineering (Core)
 - ▶ Cyber Defense Operations
- ▶ Penetration Testing and Ethical Hacking
 - ▶ Incident Response

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



Eligible for Veterans Education benefits!
Earn industry-recognized GIAC certifications throughout the program
Learn more at www.sans.edu | info@sans.edu



GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).
More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

OTHER SANS TRAINING EVENTS

SANS San Francisco 2015

San Francisco, CA | November 30 - December 5

SANS Security Leadership SUMMIT & TRAINING

Dallas, TX | December 3-10

SANS Cyber Defense Initiative 2015

Washington, DC | December 12-19

SANS Las Vegas 2016

Las Vegas, NV | January 9-14

SANS Security East 2016

New Orleans, LA | January 25-30

SANS Cyber Threat Intelligence SUMMIT & TRAINING

Alexandria, VA | February 3-10

SANS Scottsdale 2016

Scottsdale, AZ | February 8-13

SANS Northern Virginia – McLean 2016

McLean, VA | February 15-20

ICS Security SUMMIT & TRAINING

Orlando, FL | February 16-23

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING



Multi-Course Training Events sans.org/security-training/by-location/all

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers



Community SANS sans.org/community

Live Training in Your Local Region with Smaller Class Sizes



Private Training sans.org/private-training

Live Onsite Training at Your Office Location. Both in Person and Online Options Available



Mentor sans.org/mentor

Live Multi-Week Training with a Mentor



Summit sans.org/summit

Live IT Security Summits and Training

ONLINE TRAINING



OnDemand sans.org/ondemand

E-learning Available Anytime, Anywhere, at Your Own Pace



vLive sans.org/vlive

Online, Evening Courses with SANS' Top Instructors



Simulcast sans.org/simulcast

Attend a SANS Training Event without Leaving Home



OnDemand Bundles sans.org/ondemand/bundles

Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

Hotel Information

Training Campus
Anaheim Majestic Garden Hotel

900 South Disneyland Drive
 Anaheim, CA 92870
 714-234-2413

sans.org/event/anaheim-2016/location



Located across the street from the Disneyland® Resort, the Anaheim Majestic Garden Hotel is situated on 13 acres of strolling gardens with courtyards, a fountain, rose garden and koi pond. Unwind next to our sparkling outdoor heated pool and whirlpool or raise your energy level in the fitness center, family game room or video arcade/billiard room.

Special Hotel Rates Available

A special discounted rate of \$148.00 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 Feb. 4, 2016.

Top 5 reasons to stay at the Anaheim Majestic Garden Hotel

- 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 Anaheim Majestic Garden Hotel, 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 Anaheim Majestic Garden Hotel that you won't want to miss!
- 5 Everything is in one convenient location!

Registration Information

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



Register online at sans.org/event/anaheim-2016/courses

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

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.



Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	12-30-15	\$400.00	1-20-16	\$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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



To register for a SANS Anaheim Simulcast course, please visit sans.org/event/anaheim-2016/attend-remotely

Cancellation



You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by February 3, 2016 – processing fees may apply.

SANS Voucher Credit Program




Expand your training budget! Extend your fiscal year. The SANS Voucher Discount Program pays you credits and delivers flexibility. sans.org/vouchers

Open a **SANS Portal Account** today to enjoy these FREE resources:

WEBCASTS

-  **Ask The Expert Webcasts** — SANS experts bring current and timely information on relevant topics in IT Security.
-  **Analyst Webcasts** — A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.
-  **WhatWorks Webcasts** — The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.
-  **Tool Talks** — Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

-  **NewsBites** — Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals
-  **OUCH!** — The world's leading monthly free security-awareness newsletter designed for the common computer user
-  **@RISK: The Consensus Security Alert** — A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

-  **InfoSec Reading Room**
-  **Top 25 Software Errors**
-  **20 Critical Controls**
-  **Security Policies**
-  **Intrusion Detection FAQ**
-  **Tip of the Day**
-  **Security Posters**
-  **Thought Leaders**
-  **20 Coolest Careers**
-  **Security Glossary**
-  **SCORE (Security Consensus Operational Readiness Evaluation)**

sans.org/security-resources