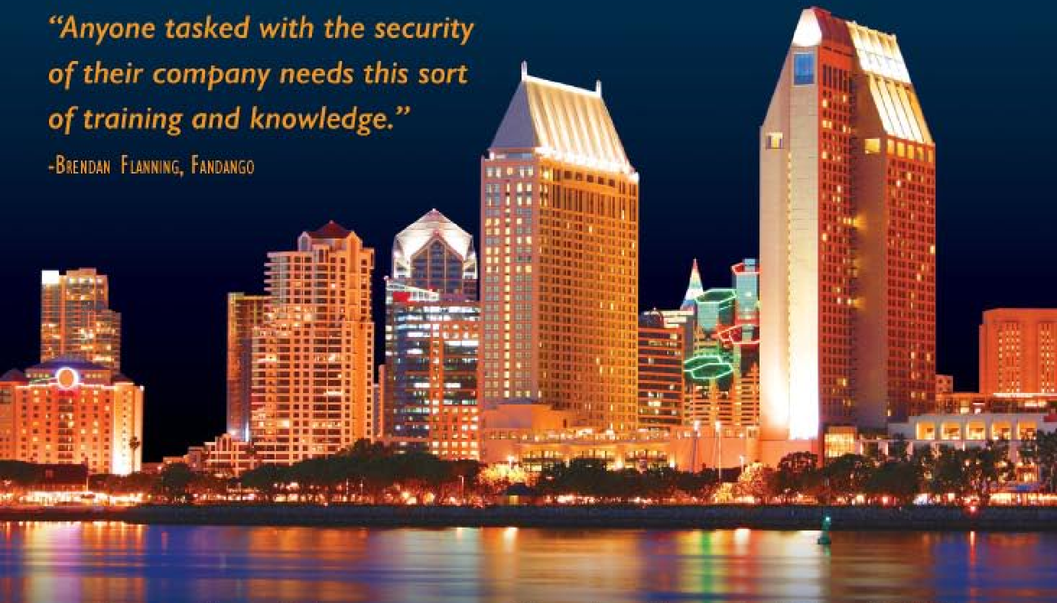
SANS Security West 2015

San Diego, CA | May 4-12

A Truly Unique
Cybersecurity Training Event

20+ courses on cyber defense, pen testing, incident response, digital forensics, and more – from the most trusted source for information security training

"Anyone tasked with the security of their company needs this sort of training and knowledge."
-Brendan Flanning, Fandango



Just a few of the courses offered at Security West 2015:

Hacker Tools, Techniques, Exploits, and Incident Handling
John Strand

Advanced Digital Forensics and Incident Response
Rob Lee

Defending Web Applications Security Essentials
Johannes Ullrich, Ph.D.

Implementing and Auditing the Critical Security Controls
James Tarala

SANS Training Program for CISSP Certification®
Paul A. Henry

Intrusion Detection In-Depth
Mike Poor

GIAC Approved Training

REGISTER AT sans.org/SecurityWest

Save $400 by paying early!
See page 33 for more details.

SAN DIEGO, CA

SANS Security West 2015

MAY 4-12, 2015

The only thing growing faster than cyber attacks today is the amount of mainstream coverage about high-profile breaches. What doesn't make the headlines are the thousands of organizations with top notch security programs that have been able to prevent or minimize the impact of business-damaging attacks. Skilled security teams implementing continuous monitoring, advanced threat detection, and advanced cyber-defense processes are the common denominator for successes across this industry.

SANS Security West 2015 features more than 20 outstanding, hands-on, immersion courses across cyber defense, pen testing, incident response, and digital forensics. SANS' world-class instructors, who are also security practitioners, will provide expert guidance and the skills you and your team can put to use immediately upon returning to the office. Beyond exceptional courses and instructors, Security West offers an abundance of interactive learning opportunities such as Bonus Sessions, panel discussions, and two NetWars Tournaments.

EMERGING TRENDS IN CYBERSECURITY

During the ***Emerging Trends*** panel discussions, we will share how cybersecurity trends are continuing to drive change in security programs. We will focus on "What Works" – what new processes, technologies, architectures, and products leading security professionals are using to effectively and efficiently deal with new threats and business demands.

PAGE 25

NETWARS

Put your security skills to the test and challenge other participants in SANS NetWars! These interactive learning scenarios enable security professionals to develop and master the real-world, in-depth skills they need to excel in their field. Which NetWars Tournament is the NetWars for you? Choose from Core NetWars, for general IT security professionals, or DFIR NetWars, which focuses on digital forensics and includes topics such as host forensics, network forensics, and malware and memory analysis.

PAGE 28

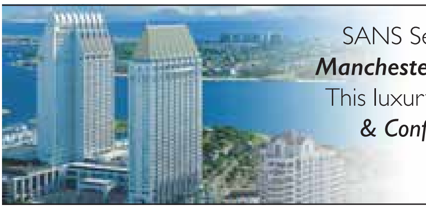
Be sure to register and pay by March 11th for a $400 tuition discount!

Have you been thinking about earning a master's degree? Then the ***SANS Technology Institute*** degree programs may be of interest to you. The SANS Technology Institute is a regionally accredited, postgraduate institution focused solely on cybersecurity education for working professionals. The brochure also provides information about earning GIAC Certification with your training.

sans.edu

giac.org

PAGE 31



SANS Security West 2015 will again be held at the fabulous ***Manchester Grand Hyatt Hotel*** on the waterfront in San Diego. This luxury hotel was recently named one of the *"Best Meeting & Conference Hotels in the U.S."* by Groups International.

PAGE 33

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

"The best training I have ever been to!"
-Bobby M.,
HP Enterprise Sevices

"Good hands on. Very knowledgeable. This training is an eye opener."
-Byron D., Danser Enterprises

"Excellent content that can be leveraged immediately!"
-William S., The Johns Hopkins University Applied Physics Laboratory

Register today for SANS Security West 2015!
sans.org/SecurityWest

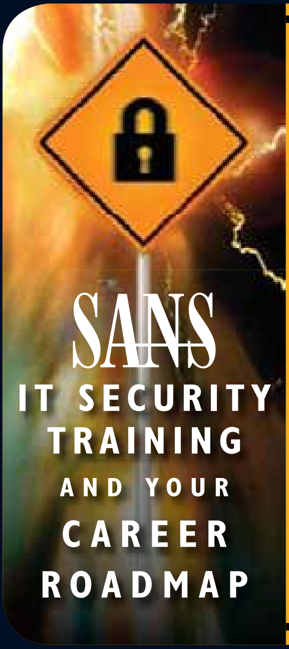
@SANSInstitute
Join the conversation:
#SecurityWest

CONTENTS

COURSES-AT-A-GLANCE

For an up-to-date course list please check the website at sans.org/SecurityWest/courses

Course	Title	Page	MON 5/4	TUE 5/5	WED 5/6	THU 5/7	FRI 5/8	SAT 5/9	SUN 5/10	MON 5/11	TUE 5/12
SEC301:	Intro to Information Security	p3		■	■	■	■	■			
SEC401:	Security Essentials Bootcamp Style	p4		■	■	■	■	■	■		
SEC440:	Critical Security Controls: Planning, Implementing, and Auditing	p24								■	■
SEC501:	Advanced Security Essentials – Enterprise Defender	p5		■	■	■	■	■	■		
SEC503:	Intrusion Detection In-Depth	p6		■	■	■	■	■	■		
SEC504:	Hacker Tools, Techniques, Exploits, and Incident Handling	p7		■	■	■	■	■	■		
SEC505:	Securing Windows with the Critical Security Controls	p8		■	■	■	■	■	■		
SEC511:	Continuous Monitoring and Security Operations ***NEW!***	p9		■	■	■	■	■	■		
SEC524:	Cloud Security Fundamentals	p24								■	■
SEC542:	Web App Penetration Testing and Ethical Hacking	p10		■	■	■	■	■	■		
SEC560:	Network Penetration Testing and Ethical Hacking	p11		■	■	■	■	■	■		
SEC561:	Intense Hands-on Pen Testing Skill Development (with SANS NetWars)	p12		■	■	■	■	■	■		
SEC566:	Implementing and Auditing the Critical Security Controls – In-Depth	p13		■	■	■	■	■			
SEC575:	Mobile Device Security and Ethical Hacking	p14		■	■	■	■	■	■		
SEC579:	Virtualization and Private Cloud Security	p15		■	■	■	■	■	■		
SEC580:	Metasploit Kung Fu for Enterprise Pen Testing	p24								■	■
FOR408:	Windows Forensic Analysis	p16		■	■	■	■	■	■		
FOR508:	Advanced Digital Forensics and Incident Response	p17		■	■	■	■	■	■		
FOR518:	Mac Forensic Analysis ***NEW!***	p18		■	■	■	■	■	■		
FOR585:	Advanced Smartphone Forensics	p19		■	■	■	■	■	■		
MGT414:	SANS Training Program for CISSP Certification®	p20		■	■	■	■	■	■		
MGT415:	A Practical Introduction to Risk Assessment	p24	■								
MGT433:	Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program	p24								■	■
MGT512:	SANS Security Leadership Essentials For Managers with Knowledge Compression™	p21		■	■	■	■	■			
DEV522	Defending Web Applications Security Essentials	p22		■	■	■	■	■	■		
ICS410:	ICS/SCADA Security Essentials	p23		■	■	■	■	■			
	NetWars Tournaments (CORE & DFIR)	p28					■	■			



SANS

IT SECURITY TRAINING AND YOUR CAREER ROADMAP

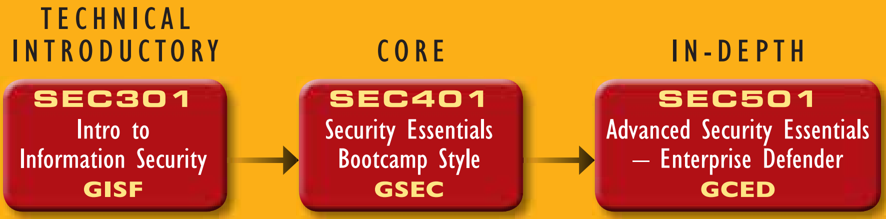
CORE COURSES

Information Security

Information security professionals are responsible for research and analysis of security threats that may affect an organization's assets, products, or technical specifications. These security professionals will dig deeper into technical protocols and specifications related to security threats than most of their peers, identifying strategies to defend against attacks by gaining an intimate knowledge of the threats.

SAMPLE JOB TITLES

- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity architect



TECHNICAL INTRODUCTORY

SEC301 Intro to Information Security **GISF**

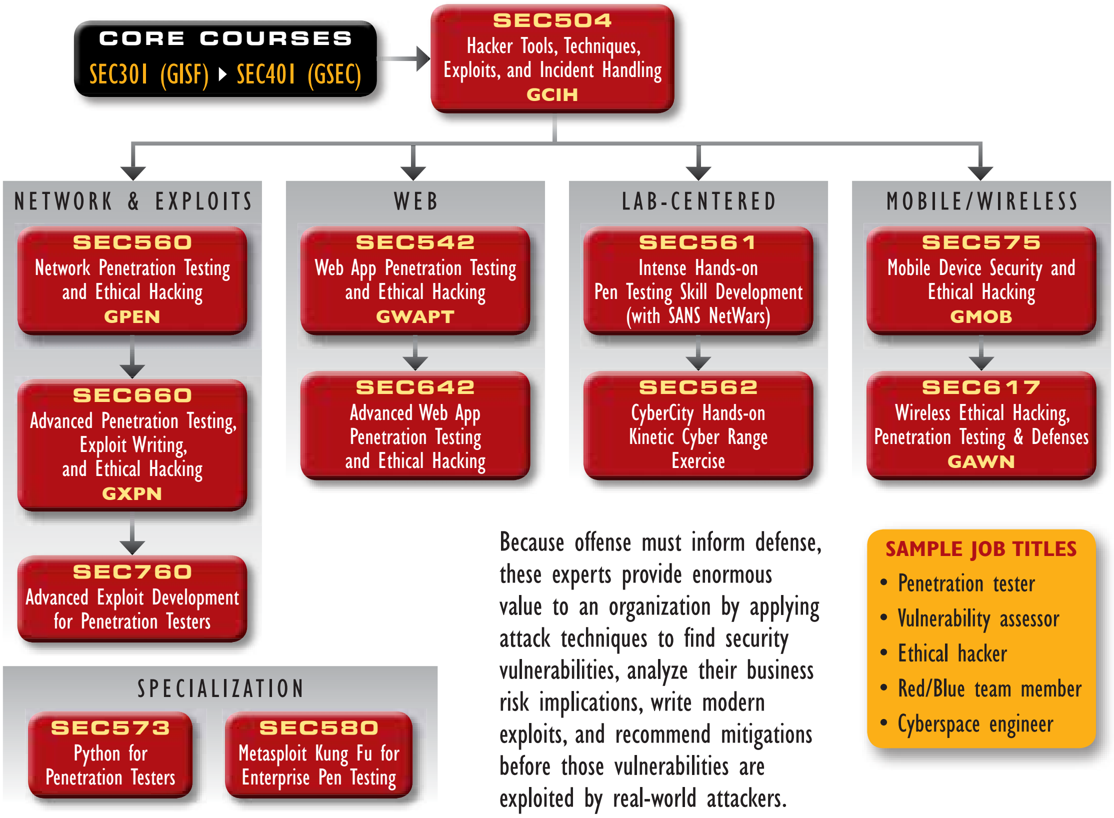
CORE

SEC401 Security Essentials Bootcamp Style **GSEC**

IN-DEPTH

SEC501 Advanced Security Essentials – Enterprise Defender **GCED**

Penetration Testing/Vulnerability Assessment



CORE COURSES

SEC301 (GISF) ▸ SEC401 (GSEC)

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

NETWORK & EXPLOITS

SEC560 Network Penetration Testing and Ethical Hacking **GPEN**

SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**

SEC760 Advanced Exploit Development for Penetration Testers

WEB

SEC542 Web App Penetration Testing and Ethical Hacking **GWAPT**

SEC642 Advanced Web App Penetration Testing and Ethical Hacking

LAB-CENTERED

SEC561 Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise

MOBILE/WIRELESS

SEC575 Mobile Device Security and Ethical Hacking **GMOB**

SEC617 Wireless Ethical Hacking, Penetration Testing & Defenses **GAWN**

SPECIALIZATION

SEC573 Python for Penetration Testers

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze their business risk implications, write modern exploits, and recommend mitigations before those vulnerabilities are exploited by real-world attackers.

SAMPLE JOB TITLES

- Penetration tester
- Vulnerability assessor
- Ethical hacker
- Red/Blue team member
- Cyberspace engineer

Risk and Compliance/Auditing/Governance

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

AUD507 Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

These experts assess and report risks to the organization by measuring compliance with policies, procedures, and standards. They recommend improvements to make the organization more efficient and profitable through continuous monitoring of risk management.

SAMPLE JOB TITLES

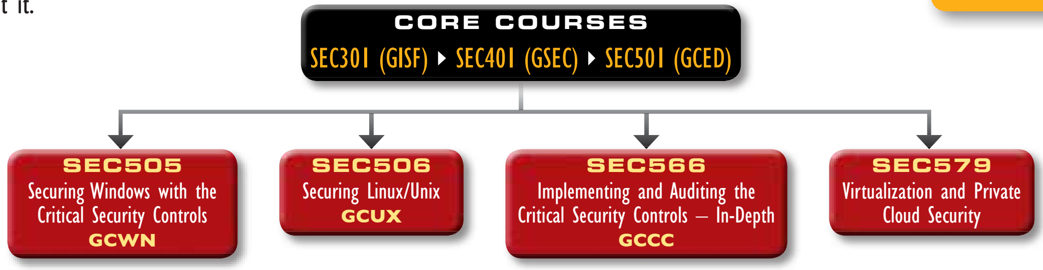
- Auditor
- Compliance officer

Network Operations Center, System Admin, Security Architecture

A Network Operations Center (NOC) is where IT professionals supervise, monitor, and maintain the enterprise network. The NOC is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC analysts work hand-in-hand with the Security Operations Center, which safeguards the enterprise and continuously monitors threats against it.

SAMPLE JOB TITLES

- System/IT administrator
- Security administrator
- Security architect/engineer



CORE COURSES

SEC301 (GISF) ▸ SEC401 (GSEC) ▸ SEC501 (GCED)

SEC505 Securing Windows with the Critical Security Controls **GCWN**

SEC506 Securing Linux/Unix **GCUX**

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

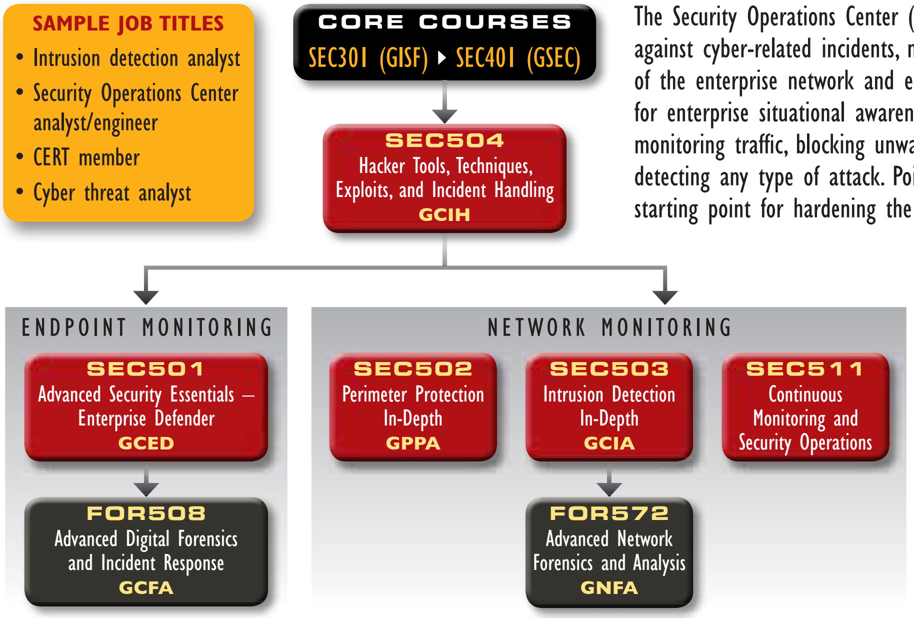
SEC579 Virtualization and Private Cloud Security

Security Operations Center/Intrusion Detection

SAMPLE JOB TITLES

- Intrusion detection analyst
- Security Operations Center analyst/engineer
- CERT member
- Cyber threat analyst

The Security Operations Center (SOC) is the focal point for safeguarding against cyber-related incidents, monitoring security, and protecting assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.



CORE COURSES

SEC301 (GISF) ▸ SEC401 (GSEC)

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

ENDPOINT MONITORING

SEC501 Advanced Security Essentials – Enterprise Defender **GCED**

FOR508 Advanced Digital Forensics and Incident Response **GCFA**

NETWORK MONITORING

SEC502 Perimeter Protection In-Depth **GPPA**

SEC503 Intrusion Detection In-Depth **GCIA**

SEC511 Continuous Monitoring and Security Operations

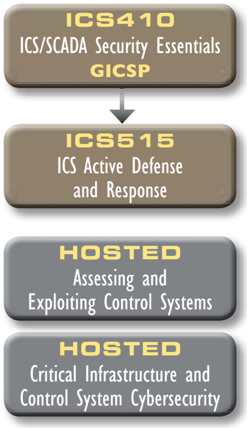
FOR572 Advanced Network Forensics and Analysis **GNFA**

Industrial Control Systems

ICS focused courses designed to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures.

SAMPLE JOB TITLES

- IT & OT Support
- IT & OT Cybersecurity
- ICS Engineer



ICS410 ICS/SCADA Security Essentials **GICSP**

ICS515 ICS Active Defense and Response

HOSTED Assessing and Exploiting Control Systems

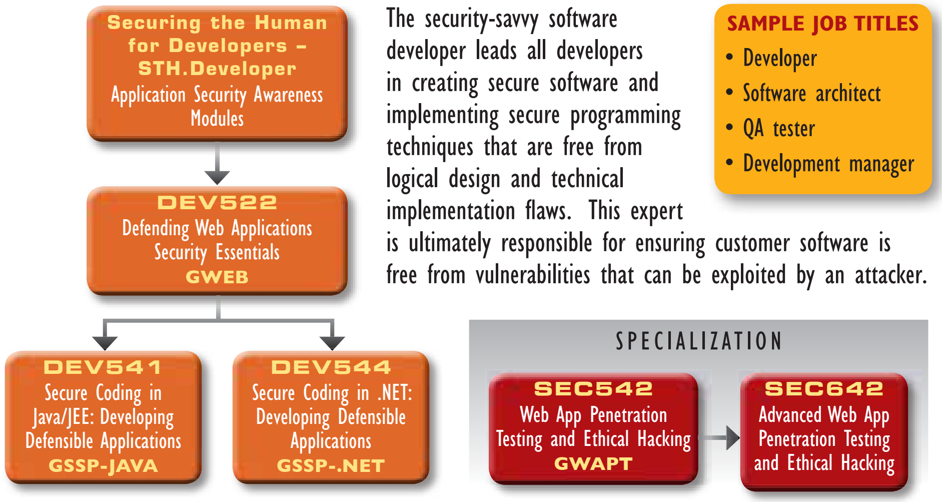
HOSTED Critical Infrastructure and Control System Cybersecurity

Development – Secure Development

The security-savvy software developer leads all developers in creating secure software and implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

SAMPLE JOB TITLES

- Developer
- Software architect
- QA tester
- Development manager



Securing the Human for Developers – STH.Developer Application Security Awareness Modules

DEV522 Defending Web Applications Security Essentials **GWEB**

DEV541 Secure Coding in Java/JEE: Developing Defensible Applications **GSSP-JAVA**

DEV544 Secure Coding in .NET: Developing Defensible Applications **GSSP-.NET**

SPECIALIZATION

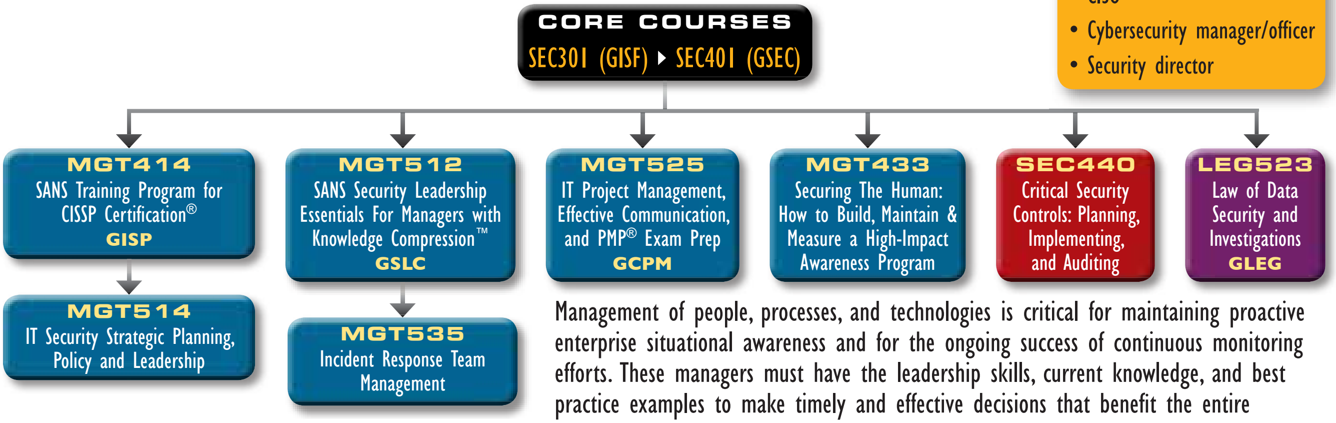
SEC542 Web App Penetration Testing and Ethical Hacking **GWAPT**

SEC642 Advanced Web App Penetration Testing and Ethical Hacking

Cyber or IT Security Management

SAMPLE JOB TITLES

- CISO
- Cybersecurity manager/officer
- Security director



CORE COURSES
SEC301 (GISF) ▸ SEC401 (GSEC)

MGT414
SANS Training Program for CISSP Certification®
GISP

MGT514
IT Security Strategic Planning, Policy and Leadership

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

MGT535
Incident Response Team Management

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

MGT433
Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program

SEC440
Critical Security Controls: Planning, Implementing, and Auditing

LEG523
Law of Data Security and Investigations
GLEG

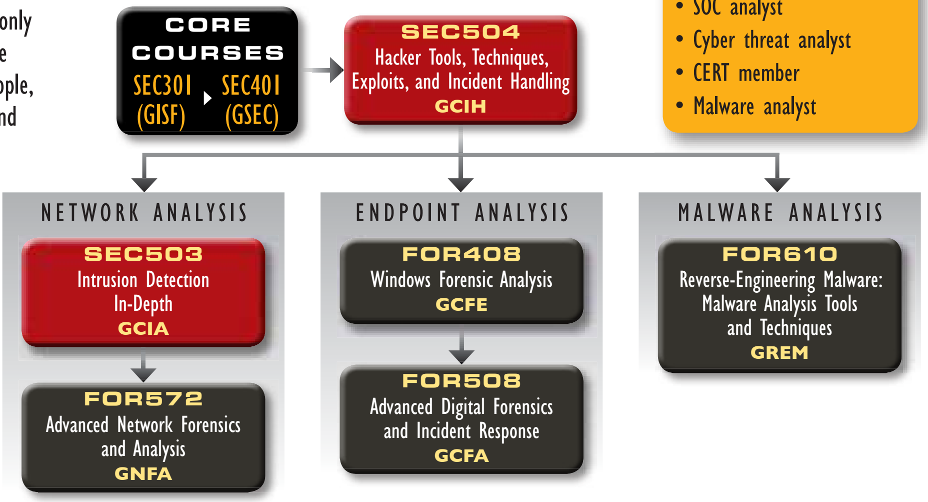
Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

Incident Response

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responders not only have to be technically astute, they must be able to handle stress under fire while navigating people, processes, and technology to help respond to and mitigate a security incident.

SAMPLE JOB TITLES

- Security analyst/engineer
- SOC analyst
- Cyber threat analyst
- CERT member
- Malware analyst



CORE COURSES
SEC301 (GISF) ▸ SEC401 (GSEC)

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

NETWORK ANALYSIS

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

ENDPOINT ANALYSIS

FOR408
Windows Forensic Analysis
GCFE

FOR508
Advanced Digital Forensics and Incident Response
GCFA

MALWARE ANALYSIS

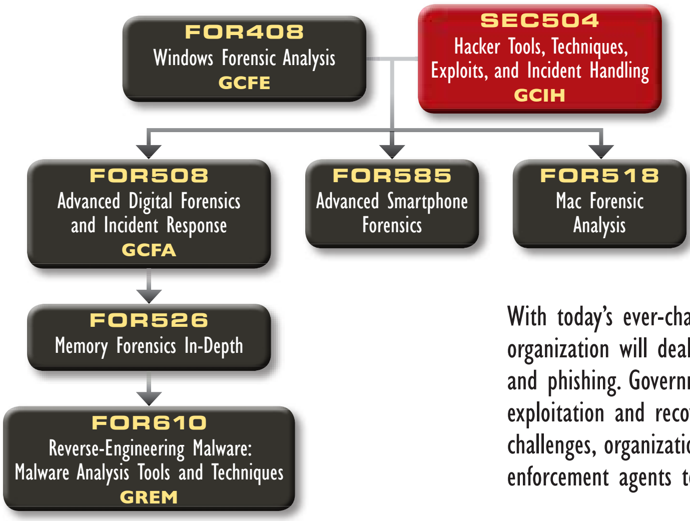
FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

SPECIALIZATION

FOR526
Memory Forensics In-Depth

MGT535
Incident Response Team Management

Digital Forensic Investigations and Media Exploitation



FOR408
Windows Forensic Analysis
GCFE

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

FOR508
Advanced Digital Forensics and Incident Response
GCFA

FOR526
Memory Forensics In-Depth

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

FOR585
Advanced Smartphone Forensics

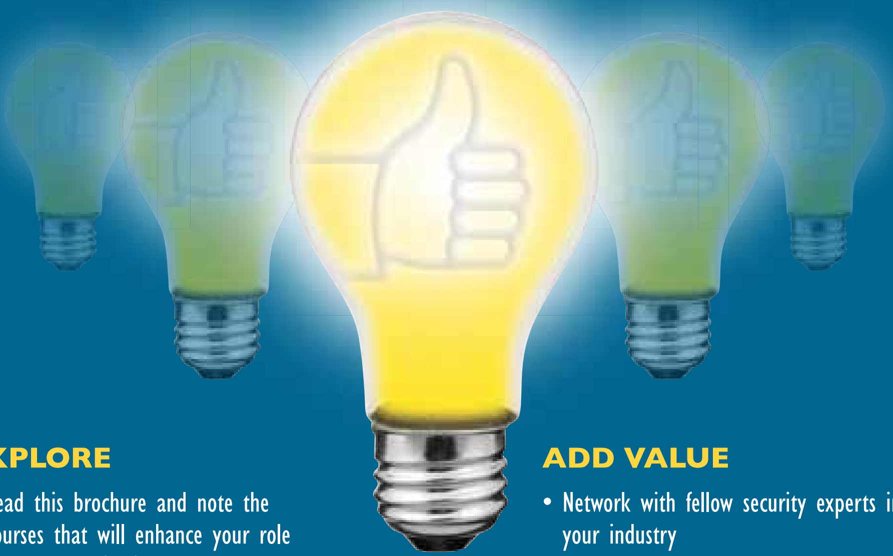
FOR518
Mac Forensic Analysis

SAMPLE JOB TITLES

- Computer crime investigator
- Law enforcement
- Digital investigations analyst
- Media exploitation analyst
- Information technology litigation support and consultant
- Insider threat analyst

With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. Government organizations also need skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

The Value of SANS Training & YOU



EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to pose to the group
- Attend SANS@Night talks and activities to glean even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career & organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER
the SANS promise:
You will be able to apply our information security training the day you get back to the office!

SANS

SECURITY 301

Intro to Information Security

Five-Day Program
Tue, May 5 - Sat, May 9
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Keith Palmgren
▶ GIAC Cert: GISF

Major Update!
Newly Released in 2015

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management.

Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss Internet Protocol, routing, Domain Name Service, and network devices. We cover the basics of cryptography, security management, and wireless technology, then we look at policy as a tool to effect change in your organization. On the final day of the course, we put it all together with an implementation of defense in-depth.

If you're a newcomer to the field of information security, this course will start you off with a solid foundation. SEC301 will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.

NOTICE: This course has been revised to incorporate practical hands-on exercises and a short practice certification test on the last day. This course will require a laptop for all classes.

GISF
giac.org

Who Should Attend

- Persons new to information technology who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and Information Security Officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

"Really interesting course – I feel as if I'm getting a great overview of security, and I now know the areas where I need more training to best get my job done."
Rachel Shaw,
Qualcomm Incorporated

"Very engaging course. I was on the edge of my seat the entire time."
-Carol Flamer, Vanguard

Keith Palmgren *SANS Certified Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice – responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570

Major Update!
Newly Released in 2015

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.

"The course SEC401 appears to have a great progressive movement from lower level to more in-depth security practices, and is a great way to refresh topics learned while covering new technology."
-Angela Stewart, Regions Financial Corp.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

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

"This is the third time I've taken SEC401. Each time I've taken something new away, and have been able to use it in my day to day job."
-Jennifer Bakowski, John Hancock Financial Services

Bryan Simon *SANS Instructor*

With more than 20 years of experience in information technology and infosec, Bryan Simon is an internationally recognized expert in cybersecurity. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity, and has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. Bryan has received recognition for his work in I.T. Security, and was most recently profiled by McAfee (part of Intel Security) as an I.T. Hero. Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program.

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Bryce Galbraith

- GIAC Cert: GCED
- STI Master's Program

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials - Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Of course, despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

giac.org

sans.edu

"Good introduction and hands-on experience with a variety of tools!"
-Carrie Crot, DOJ

"A very good thoughtful and practical understanding of security, something everyone in IT should get."
-Paul Godard, OPC

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

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he holds several security certifications and speaks at conferences around the world. @brycegalbraith

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/SecurityWest/courses

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Mike Poor

- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570

"This course provides real-world content and perspectives, data, and tools. The instructor is very knowledgeable and is a great educator."
-George Diolamou, Jacob's Engineering

"Awesome course! Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

"The amount of knowledge and experience that Mike has, I don't think you could get that from any other organization other than SANS."
-Hayley Roberts, MOD

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 (all levels), system, and security analysts
- Network engineers/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'll 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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Mike Poor *SANS Senior Instructor*

Mike Poor is a founder and senior security analyst for the Washington, DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is on intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling "Snort" series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center. @Mike_Poor

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570

"SEC504 is awesome! Everything included in this course is very useful in my job as a security professional!"
-Vereleo Bateo, KCG Holdings, Inc.

"John made me feel more confident and less stressed at the beginning of the course by making it clear that he's here to help."
-Bruno Leblanc, Ubisoft

"This course is very beneficial and will sharpen your skills and then some."
-Robert Delizio, Federal Reserve Bank of New York

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

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.

giac.org

sans.edu

sans.org/
cyber-guardian

sans.org/8570

John Strand *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464 and the co-author for SEC580. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing. @strandjs

SECURITY 505

Securing Windows with the Critical Security Controls

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- STI Master's Program
- Cyber Guardian

How can we deal with pass-the-hash attacks, token abuse, administrator account compromise, and lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that lead to malware infections? These are tough problems, but we tackle them in SEC505.

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defenses against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is useful, but there is no simple patch against their abuse. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future. This requires more than just reactive patch management – we need to proactively design security into our systems and networks. That is what SEC505 is about.

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy hardening and PowerShell scripting. Learning PowerShell is probably the single best new skill for Windows users, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills, so knowing PowerShell is a great way to make your resume stand out. This course devotes an entire day to PowerShell, but we start with the basics so you do not need any prior scripting experience.

This is a fun course and a real eye-opener even for Windows administrators with years of experience. If you wish, you can get the PowerShell scripts now for this course from **http://cyber-defense.sans.org/blog** (go to the Downloads link). All of the tools are in the public domain.

giac.org

sans.edu

sans.org/
cyber-guardian

Who Should Attend

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the 20 Critical Security Controls
- Anyone implementing the Australian Directorate's Four Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- Anyone who needs to prevent malware infections

"SEC505 course content is excellent. In-class activities were very valuable. Very good teaching skills and knowledge."
-Jesus Perez,
Texas A&M University

"I have been to other windows training, but never one with a focus on security – this has been an eye-opening experience. I hope to attend more events like this in the future."
-Dewayne Wasson,
Kellogg Company

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS' week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS' projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. Jason blogs about Windows Security Issues on the SANS Windows Security Blog (http://blogs.sans.org/windows-security) @JasonFossen

SECURITY 511

Continuous Monitoring and Security Operations

NEW

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

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

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

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

"When students walk out, they have a list of action items in hand for making their organization one of the most effective vehicles for frustrating adversaries."
-Eric Conrad and Seth Misenar, SANS

"The material in SEC511 is excellent, and I appreciate the background/pen test material build up to defense. Good defense understands offense."
-Kenneth Hall, BCBSMS

Seth Misenar *SANS Principal Instructor*

Seth Misenar 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. @sethmisenar

SANS

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

- GIAC Cert: GWAPT
- Cyber Guardian
- STI Master's Program

Web applications play a vital role in every modern organization. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data.

Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so, not surprisingly, every major industry study finds that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations.

Who Should Attend

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

giac.org

sans.edu

sans.org/
cyber-guardian

"Web app assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."
-James Kelly,
Blue Canopy LLP

"With the infinite tools used for web app penetration, SEC542 helps you understand/use the best tools for your environment."
-Linh Sithihao, UT
Southwestern Medical Center

"SEC542 is an essential course for application security professionals."
-John Yamich, Exact Target

Eric Conrad *SANS Principal Instructor*

Eric Conrad is lead author of the book "The CISSP Study Guide." Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com. @eric_conrad

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this duty head-on.

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

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

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

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

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

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

giac.org

sans.edu

sans.org/
cyber-guardian

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

"I had a great time. SEC560 has tons of useful material and techniques. As with all SANS training, I leave knowing that I can apply this as soon as I am back at work."
-Benjamin Bagby, XE.Com

"This training is extremely important, given the nature of DOD networks. The best answers to compromising a system are likely going to be the hardest to implement."
-David Poulin,
7th Cyber Protection Brigade

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org) @mikemurr

SECURITY 561

Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered SEC561: Intense Hands-on Pen Testing Skill Development from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time on in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Who Should Attend

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening and penetration testing.
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators.
- Incident response analysts who want to better understand system attack and defense techniques.
- Forensic analysts who need to improve their skills through experience with real-world attacks.
- Penetration testers seeking to gain practical hands-on experience for use in their own assessments.
- Red team members who want to build their hands-on skills, and blue team members who want to better understand attacks and defend their environments.

"This class really forces you to think and the format rewards your hard work and dedication to finding the solutions."
-Michael Nutbrown, Solers, Inc

"80% hands-on is intense and the best way to build on previous pen-testing-focused SANS courses."
-Timothy McKenzie, Dell/Secureworks

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joshwrIght

SECURITY 566

Implementing and Auditing the Critical Security Controls – In-Depth

SANS

Five-Day Program
Tue, May 5 - Sat, May 9
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala

- GIAC Cert: GCCC
- STI Master's Program

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.

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.

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

giac.org

sans.edu

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

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

"SEC566 is a very comprehensive course, and the collections of lists are useful, informative tools that can be moved into the real day-to-day job."
-Henry Jiang

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based in 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. @isaudit

SANS

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Christopher Crowley

- GIAC Cert: GMOB
- STI Master's Program

giac.org

sans.edu

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient e-mail access as well by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **The high probability of device loss or theft, and more**

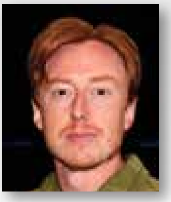
Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From evaluating the network activity generated by mobile applications to mobile code analysis, from exploiting the weaknesses in common mobile applications to conducting a full-scale mobile penetration test, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

> "Once again, SANS has exceeded my expectations and successfully refocused my view of threats and risks. I recommend this course because it is very enlightening."
> -Charles Allen, EM Solutions

> "This course was everything I've been looking for over the last few years. Job well done on putting the course together."
> -Troy Wojewoda, Huntington Ingalls Industries



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. Mr. Crowley is the course author for SANS Management 535 - 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

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Dave Shackleford

One of today's most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management for virtualized systems. There are even security benefits of virtualization – easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructures.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds – internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

"Dave is an excellent teacher and communicator. He made a highly technical course interesting and the overall experience was thoroughly enjoyable!!"
-Wayne Rosen, Adnet Systems, Inc.

Who Should Attend

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

"Overall, it's a great course! The exploits and PoC are cutting edge!! This is the future of IT and security knowledge is power!"
-Joe Marshall, Exelon

"Great course! Anyone involved with managing virtual system environments will benefit from taking SEC579."
-Randall Riley, Defense Security Services

Dave Shackleford *SANS Senior Instructor*

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book *Virtualization Security: Protecting Virtualized Environments*, as well as the coauthor of *Hands-On Information Security* from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. @daveshackleford

FORENSICS 408

Windows Forensic Analysis

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury
- GIAC Cert: GCFE
- STI Master's Program

digital-forensics.sans.org

Master Computer Forensics. What Do You Want to Uncover Today?

Every organization will deal with cyber-crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

FOR408: Windows Forensic Analysis focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 7 artifacts.

This course utilizes a brand-new Windows 8.1-based realistic case exercise for which it took over 6 months to create the data. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. Our development team has created an incredibly realistic scenario. The brand new case workbook, will detail the step-by-step each investigator could follow to examine the latest technologies including Windows 8.1.

FIGHT CRIME. UNRAVEL INCIDENTS...
ONE BYTE AT A TIME

giac.org

sans.edu

Who Should Attend

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

"FOR408 is based on real scenarios that are likely to occur again. The most up-to-date training I have received."
-Martin Heyde, UK Ministry of Defence

"FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations."
-Nathan Lewis, KPMG

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 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 sixty 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

FORENSICS 508

Advanced Digital Forensics and Incident Response

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

- GIAC Cert: GCFA
- STI Master's Program
- Cyber Guardian
- DoDD 8570

DAY 0: A 3-letter government agency contacts you to say critical information was stolen from 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.

Who Should Attend

- IT 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 looking to take their skills to the next level

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 remediate the incident rapidly.

FOR508: will help your incident response team to determine:

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

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

During a targeted attack, an organization needs the best incident response team in the field. **FOR508:Advanced Digital Forensics and Incident Response** will train you and your team to be ready to respond, detect, scope, and stop intrusions and data breaches.

**GATHER YOUR INICDENT RESPONSE TEAM –
IT'S TIME TO GO HUNTING**

digital-forensics.sans.org

giac.org

sans.edu

sans.org/
cyber-guardian

sans.org/8570

"Extremely valuable course overall, and brings essential topics into one. The course covers an extensive amount of topics with excellent reference material."
-Edgar Zayas,
U.S. Securities and Exchange Commission

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy, 2nd Edition.* Rob is also co-author of the MANDIANT threat intelligence report "M-Trends: The Advanced Persistent Threat." @robtlee & @sansforensics

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/SecurityWest/courses

FORENSICS 518

Mac Forensic Analysis

NEW

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Sarah Edwards

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, FOR585 alumni looking to round out their forensic skills

digital-forensics.sans.org

FORENSICATE DIFFERENTLY!

FOR518: Mac Forensic Analysis will teach you:

- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) file system 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.

"Valuable information to take back to work with me, as well as hands-on testing examples."
-Carol Jones

"Best of any course I've ever taken. I love the idea of being able to bring home and review."
-Eric Koebelen, Incident Response US

Sarah Edwards *SANS 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, counter-intelligence, counter-narcotic, and counter-terrorism. 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, BsidesNOLA, 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

FORENSICS 585

Advanced Smartphone Forensics

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Heather Mahalik

DFIR
digital-forensics.sans.org

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

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

Who Should Attend

- Experienced digital forensics examiners who want to extend their knowledge and experience to forensics analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and what files they accessed
- Information security professionals who respond to data breach incidents and intrusions
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents or detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- IT auditors who want to learn how smartphones can expose sensitive information
- Graduates of SANS SEC575, FOR408, FOR508, or FOR518 who want to take their skills to the next level

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

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

"Examiners who are tasked with acquiring and analyzing data, this course is a must!"
-Helena Polend,
VA Dept of Forensic Science

"This is the most advanced mobile device training that I know of and is greatly needed. It is currently the only course being taught at this level!"
-Scott McNamee DoS/CACI

Heather Mahalik *SANS Certified Instructor*

Heather Mahalik is a project manager for Ocean's Edge, where she uses her experience to manage projects focused on wireless cyber security and mobile application development. Heather has over 12 years of experience in digital forensics, vulnerability discovery of mobile devices, application reverse engineering and manual decoding. She is currently a certified instructor for the SANS Institute and is the course lead for FOR585, Advanced Smartphone Forensics. Previously, Heather led the mobile device team for Basis Technology, where she led the mobile device exploitation efforts in support of the U.S. Government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high profiles cases. Heather co-authored Practical Mobile Forensics and various white papers, presented at leading conferences, and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather maintains www.smarterforensics.com where she blogs and hosts work from the digital forensics community. @HeatherMahalik

MANAGEMENT 414

SANS Training Program for CISSP Certification®

Six-Day Program
Tue, May 5 - Sun, May 10
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Paul A. Henry
- GIAC Cert: GISP
- DoDD 8570

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

"MGT414 offers a good top-level look at the information — it helps to know what to focus on."
-Paul Gunnerson, U.S. Army

"Great course and well worth it if you are considering taking the CISSP exam."
-David Raymond, U.S. Army

Over the past four years, 98% of all respondents who took the SANS Training Program passed the CISSP® Certification Exam. This compares to a national average of around 70% for other prep courses.

MGT414: SANS Training Program for CISSP® Certification is an accelerated review course designed to prepare you to pass the exam.The course takes into account the updates to the CISSP® exam and has been constantly updated to keep track of any changes and updates to the exam since then.

This course assumes that students have a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge as determined by (ISC)². Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of network security.

After completion of this course, students will have a strong working knowledge of the 10 domains of knowledge and be better placed to pass the exam.

Who Should Attend

- Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)².
- Managers who want to understand the critical areas of network security.
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 domains.
- Security professionals and managers looking for practical ways to apply the 10 domains of knowledge to their current activities

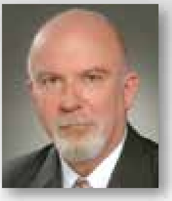
You Will Be Able To:

- Understand the 10 domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the 10 domains of knowledge
- Apply the skills learned across the 10 domains to solve security problems when you. return to work

giac.org

sans.org/8570

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



Paul A. Henry *SANS Senior Instructor*

Paul Henry is a Senior Instructor with the SANS Institute and 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 (USA), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Tue, May 5 - Sat, May 9
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: G. Mark Hardy

- GIAC Cert: GSLC
- STI Master's Program
- DoDD 8570

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.

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

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.

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

> "MGT512 gives a good understanding of what knowledge our employees need to have to be successful."
> -Teddie Steele, State Department of FCU

giac.org

sans.edu

sans.org/8570

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!

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 worldwide. 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. @g_mark

DEVELOPER 522

Defending Web Applications Security Essentials

SANS

Six-Day Program
Tue May 5 - Sun May 10
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.
- GIAC Cert: GWEB
- STI Master's Program

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues, and to infrastructure security professionals who have an interest in better defending their web applications.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with PCI requirements

"What you don't know about web app defense is most likely killing you and you wouldn't know it."
-Michael Malarkey, Bank of America

"This course really proved to me that ignorance is bliss. I learned a lot that I could immediately take back to the office."
-Shawn Shirley, Ferrum College

giac.org

sans.edu

Johannes Ullrich, Ph.D. *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. 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. His daily podcast summarizes current security news in a concise format. @johullrich

INDUSTRIAL CONTROL SYSTEMS 410

ICS/SCADA Security Essentials

Five-Day Program
Tue May 5 - Sat, May 9
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Graham Speake
▸ GIAC Cert: GICSP

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

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

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

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

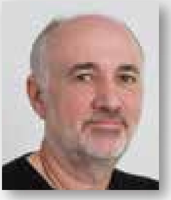
giac.org

Who Should Attend

- The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:
- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

"This training has definitely empowered me some more with knowledge above standards. I believe that if I apply the leaning I received here, I will be able to perform as a network engineer & CS-IT with more expertise."
-Robin U. Familara, CGI

"Very satisfied with ICS410, and the instructor was very knowledgeable and great at balancing group backgrounds (IT vs. SCADA)."
-Chad Slater,
The Dow Chemical Company



Graham Speake *SANS Instructor*

Graham Speake is Vice President and Chief Product Architect at NexDefense. Previously to NexDefense, he was Principal Systems Architect for Yokogawa Electric Corporation, ISCI Marketing Chair, and an IEC62443 editor. Graham is an engineer with over 30 years' experience, the last 16 of which have been in the industrial cyber security arena for both end user companies and vendors. Graham has spent 10 years in BP looking at control systems security in both upstream and downstream business areas. Additionally, he has 5 years' experience in designing safety systems at Industrial Control Services. Graham is the author of a number of books and frequent contributor to magazine articles.

SEC440: Critical Security Controls: Planning, Implementing & Auditing

Two-Day Course | Mon, May 11 - Tue, May 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Recommended

Instructor: James Tarala

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

SEC524: Cloud Security Fundamentals

Two-Day Course | Mon, May 11 - Tue, May 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required

Instructor: Paul A. Henry

Many organizations today are feeling pressure to reduce IT costs and optimize IT operations. Cloud computing is fast emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities, and many more IT functions. A staggering number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

The first fundamental issue is the loss of hands-on control of system, application and data security. Many of the existing best-practice security controls that information security professionals have come to rely on are not available in cloud environments, are available but stripped down in many ways, or cannot be controlled by security teams. Security professionals must become heavily involved in the development of contract language and service-level agreements when doing business with cloud service providers (CSPs). Compliance and auditing concerns are compounded. Control verification and audit reporting within CSP environments may be less in-depth and frequent than that required by audit and security teams.

SEC524: Cloud Security Fundamentals starts out with a detailed introduction to the various delivery models of cloud computing, ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represent an entirely separate set of security conditions to consider, especially when coupled with various cloud types, including public, private and hybrid. An overview of security issues within each of these models will be covered with an in-depth discussion of the risks involved. The course will go in-depth on architecture and infrastructure fundamentals for private, public and hybrid clouds, including a wide range of topics such as patch and configuration management, virtualization security, application security and change management. Policy, risk assessment and governance within cloud environments will also be covered, with recommendations for both internal policies and contract provisions. This path leads to a discussion of compliance and legal concerns.The first day will wrap up with several fundamental scenarios for students to evaluate.

SEC580: Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Mon, May 11 - Tue, May 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required

Instructor: Bryce Galbraith

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit, are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an Open Source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

MGT415: A Practical Introduction to Risk Assessment

One-Day Course | Mon, May 4 | 9:00am - 5:00pm | 6 CPEs | Laptop Required

Instructor: James Tarala

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

MGT433: Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Two-Day Course | Mon, May 11 - Tue, May 12 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed

Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The simplest way for cyber attackers to hack into your organization is to target your employees. Unless, of course, you take the steps necessary to stop them. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers, as well. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

SANS@NIGHT EVENING TALKS

EMERGING TRENDS IN CYBERSECURITY

"I was not predicting the future, I was trying to prevent it."

-Ray Bradbury

As technology advances and threats evolve, it's imperative to stay abreast of Emerging Trends in cybersecurity. At SANS Security West, leading security experts tackle these developments in interactive panel discussions with analysis and insight into the coming year in security, pen testing, and digital forensics.

KEYNOTE: Emerging Trends in Cybersecurity 2015 *John Pescatore*

Going by the headlines in 2014, the news for cybersecurity was all negative: more stories about companies suffering more and larger breaches. Be sure not to miss John Pescatore's keynote address where he focuses on trends in threat vectors as well as developments in business and technology that impact approaches to security including staffing, vendors, and a review of "What Works."

The Future of Cyber Defense *Paul A. Henry*

We are working in an environment where large scale breaches have become all too commonplace – sadly most often as a result of not following the very basics in good network security. The run rate of new, unique instances of malware is greater than two instances per second. At least one AV vendor has openly given up on traditional solutions. Brick & mortar companies are being forced into the cloud in spite of the security risks or they risk financial ruin. This session discusses the future of cyber defense to equip cyber defenders to meet these challenges. Subject matter will include the evolution of flaw remediation to virtual patching, developments in cyber intelligence with automated response, and advances in cloud security.

Emerging Trends in DFIR

Lightning Talks with Rob Lee, Chad Tilbury, Heather Mahalik, Paul Henry, and Sarah Edwards

Join Rob Lee, Chad Tilbury, Heather Mahalik, Paul Henry, and Sarah Edwards as they each unveil their top Emerging Trends in DFIR in a series of lively, hard-hitting lightning talks (8-10 minutes each). Get a glimpse into the near future for incident response and digital forensics.

Emerging Trends in Pen Testing: The Coolest New Trends and How They Rocked Your World

Panelists include John Strand, Eric Conrad, Chris Crowley, and Mike Murr

The right tool – or lack thereof – can make or break a pen test. Our panelists share the coolest tool, or feature of a tool, to rock their worlds in the last 12 months, and how they used it to great advantage in a pen test. We'll look at trends and practical ways pen testers can take advantage of these new advances in our field to do amazing things in helping organizations understand and manage their risk.

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.

The Internet of Evil Things

Johannes Ullrich, PhD

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

The 13 Absolute Truths of Security

Keith Palmgren

Keith Palmgren has identified thirteen absolute truths of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

Everything They Told Me About Security Was Wrong

John Strand

If you were to believe the vendors and the trade shows, you would think everything was OK with IT security. You would think AV works. You would think plug and play IDS was effective. You would think that Data Loss Prevention would prevent data loss. Why then, is it, that very large organizations are still getting compromised? Organizations with very large budgets and staff, still get compromised in advanced and persistent ways. Something is very wrong in this industry. Let's find out what is wrong and how we can fix it.

Debunking the Complex Password Myth

Keith Palmgren

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves, and even for their children.

SANS@NIGHT EVENING TALKS

SOC and Continuous Monitoring

Seth Misenar and Eric Conrad

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course: SANS SEC511: Continuous Monitoring and Security Operations.

Enterprise PowerShell for Remote Security Assessment

James Tarala

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Not only are organizations attempting to automate their assessments, the need is becoming more pressing to perform assessments centrally against large numbers of enterprise systems. Forensic analysts, incident handlers, penetration testers, and auditors all regularly find themselves in situations where they need to remotely assess a large number of systems through an automated set of tools. Microsoft's PowerShell scripting language has become the defacto standard for many organizations looking to perform this level of distributed automation. In this presentation James Tarala, of Enclave Security, will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large scale Windows security assessments.

Why Our Defenses Are Failing Us. One Click Is All It Takes.

Bryce Galbraith

Organizations are spending unprecedented amounts of money in an attempt to defend their assets...yet all too often, one click is all it takes for everything to come toppling down around them. Every day we read in the news about national secrets, intellectual property, financial records, and personal details being exfiltrated from the largest organizations on earth. How is this being done? How are they bypassing our defenses (e.g. strong passwords, non-privileged accounts, anti-virus, firewalls/proxies, IDS/IPS, logging, etc.)? And most importantly, what can we do about it? A keen understanding of the true risks we face in today's threatscape is paramount to our success.

Windows Exploratory Surgery with Process Hacker

Jason Fossen

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware. **http://processhacker.sourceforge.net**

The CORE NetWars and DFIR NetWars Tournaments will be held simultaneously at Security West 2015!

NETWARS

CORE NETWARS TOURNAMENT

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

Who Should Attend

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center staff

In-Depth, Hands-On InfoSec Skills – Embrace the Challenge – CORE NetWars

DFIR NETWARS TOURNAMENT

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

Who Should Attend

- Digital forensic analysts
- Forensic examiners
- Reverse-engineering and malware analysts
- Incident responders
- Law enforcement officers, federal agents, and detectives
- Security Operations Center analysts
- Cyber crime investigators
- Media exploitation analysts

Challenge Yourself Before the Enemy Does – DFIR NetWars

Both NetWars competitions will be played over two evenings: May 8-9, 2015

Prizes will be awarded at the conclusion of the tournaments.

REGISTRATION IS FREE BUT LIMITED

for students attending any long course at Security West (NON-STUDENT'S ENTRANCE FEE IS $1,249).

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

GIAC

How Are You Protecting Your

Data? Network? Systems? Critical Infrastructure?

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

Learn more about GIAC and how to get certified at **www.giac.org**

DoDD 8570

sans.org/8570

DoDD 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 has the most certifications that meet the requirements for Technical, Management, CND, and IASAE classifications. SANS courses prepare you to take a GIAC exam.

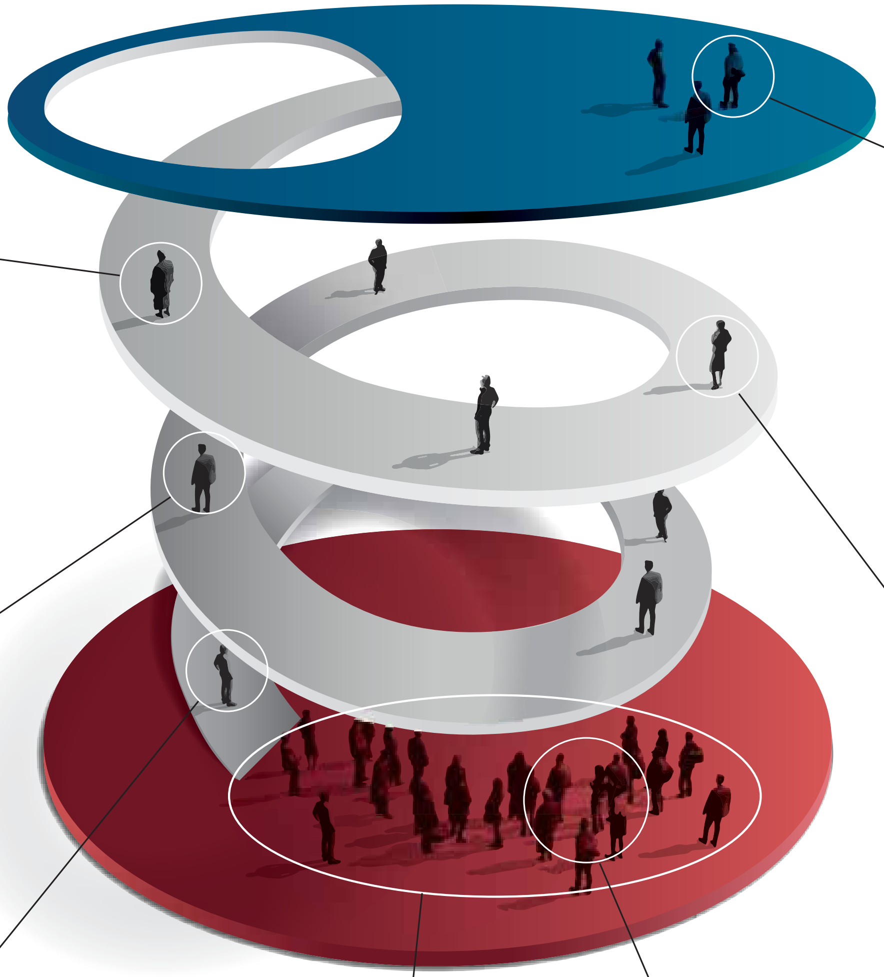
For more information about DoDD 8570:

Contact the DoDD 8570 Information Assurance Workforce Improvement Program Office at **http://iase.disa.mil/iawip/Pages/index.aspx**

Contact **8570@sans.org** or call customer support at **301-654-7267**.

EDUCATING THE WORLD IN CYBERSECURITY

Protecting data has never been more important. As attackers become more sophisticated and determined, preventing a breach requires a honed skillset of real-world knowledge and capabilities. SANS is a one-stop information-security education provider, featuring hands-on training, GIAC certification, and security awareness and graduate programs. SANS' world-class instructors and proven curricula will empower you with the ability to protect and defend your vital systems and data.



Cyber Guardian

Designed for elite teams of technical security professionals whose roles include securing systems, reconnaissance, counterterrorism, and counter hacks

sans.org/cyber-guardian

SANS NetWars

Test hands-on technical skills in a safe environment to be prepared when a real incident occurs

sans.org/netwars

SANS Training

Hands-on security training for professionals just starting in security up to seasoned professionals

Training courses are delivered at live events and online

sans.org

SANS Security Awareness

Everything your organization needs for an effective security awareness program

securingthehuman.org

SANS Technology Institute

A regionally accredited postgraduate institution focused solely on information security education for working professionals

sans.edu

GIAC Certification

Credential the technical skills and knowledge of your security professionals

giac.org

SANS CyberTalent

Assess the skills and aptitude of security professionals to inform hiring decisions

sans.org/cybertalent

FUTURE SANS TRAINING EVENTS

10TH ANNUAL **ICS Security** SUMMIT – ORLANDO 2015
Orlando, FL | February 22 - March 2 | #SANSICS

SANS **DFIR Monterey** 2015
Monterey, CA | February 23-28 | #DFIRMonterey

SANS **Cyber Guardian** 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS **Northern Virginia** 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS **Houston** 2015
Houston, TX | March 23-28 | #SANSHouston

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

SANS **Pen Test Austin** 2015
Austin, TX | May 18-23 | #PenTestAustin

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS **Rocky Mountain** 2015
Denver, CO | June 22-27 | #SANSRockyMtn

Visit sans.org for a complete schedule.

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

SANS SECURITY WEST 2015

Hotel Information

Training Campus

Manchester Grand Hyatt San Diego

One Market Place
San Diego, CA 92101
sans.org/SecurityWest/location

Discover the culture and beauty of San Diego right outside your door at the Manchester Grand Hyatt. Wake to the sun sparkling off San Diego Bay, indulge in breakfast on the boardwalk at Sally's, enjoy a little shopping at Seaport Village or take a coastal cruise. This luxury hotel was recently named one of the *"Best Meeting & Conference Hotels in the U.S."* by Groups International.

Special Hotel Rates Available

A special discounted rate of $215.00 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 April 13, 2015.

Top 5 reasons to stay at the Manchester Grand Hyatt

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 Manchester Grand Hyatt, 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 Manchester Grand Hyatt that you won't want to miss!
5. Everything is in one convenient location!

SANS SECURITY WEST 2015

Registration Information

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

Register online at sans.org/SecurityWest/courses

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

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

Use code **EarlyBird15** when registering

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	3/11/15	$400.00	4/8/15	$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)*

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

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

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

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 April 15, 2015 – 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

Sign up for a **SANS Portal Account** and receive free webcasts, newsletters, the latest news and updates, and many other free resources.

sans.org/portal

SANS NewsBites

Join over 200,000 professionals who subscribe to this high-level, executive summary of the most important news and issues relevant to cybersecurity professionals. Delivered twice weekly. Read insightful commentary from expert SANS instructors.

InfoSec Reading Room

Computer security research and whitepapers

Security Policies

Templates for rapid information security policy development

Top 25 Software Errors

The most widespread and critical errors leading to serious vulnerabilities

OUCH!

OUCH! is the world's leading, free security awareness newsletter designed for the common computer user. Published every month and in multiple languages, each edition is carefully researched and developed by the SANS Securing The Human team, SANS instructor subject-matter experts and team members of the community. Each issue focuses on a specific topic and actionable steps people can take to protect themselves, their family and their organization.

Webcasts

SANS Information Security Webcasts are live broadcasts by knowledgeable speakers addressing key issues in cybersecurity, often in response to breaking news about risks. Gain valuable information on topics you tell us are most interesting!

Critical Security Controls

Consensus guidelines for effective cyber defense

Industry Thought Leadership

In-depth interviews with the thought leaders in information security and IT

Intrusion Detection FAQ

The Internet's most trusted site for vendor-neutral intrusion detection information

@RISK: The Consensus Security Alert

@RISK provides a reliable weekly summary of:

1. Newly discovered attack vectors
2. Vulnerabilities with active new exploits
3. Insightful explanations of how recent attacks worked and other valuable data

A key purpose of @RISK is to provide data that will ensure that the Critical Controls continue to be the most effective defenses for all known attack vectors.