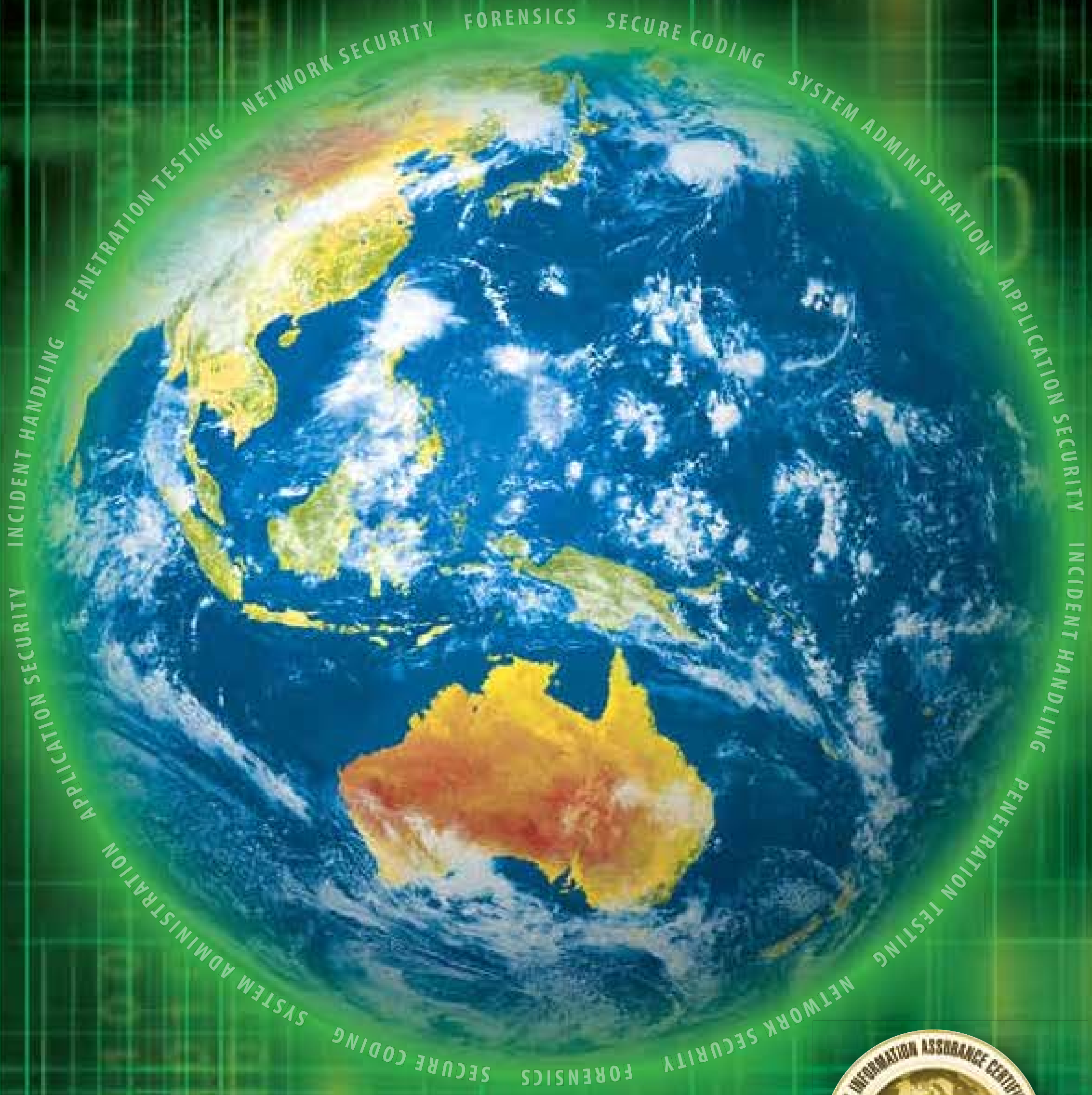
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS

2014 ASIA PACIFIC Course Catalog v2

Australia India Indonesia Japan Korea Malaysia Singapore Thailand



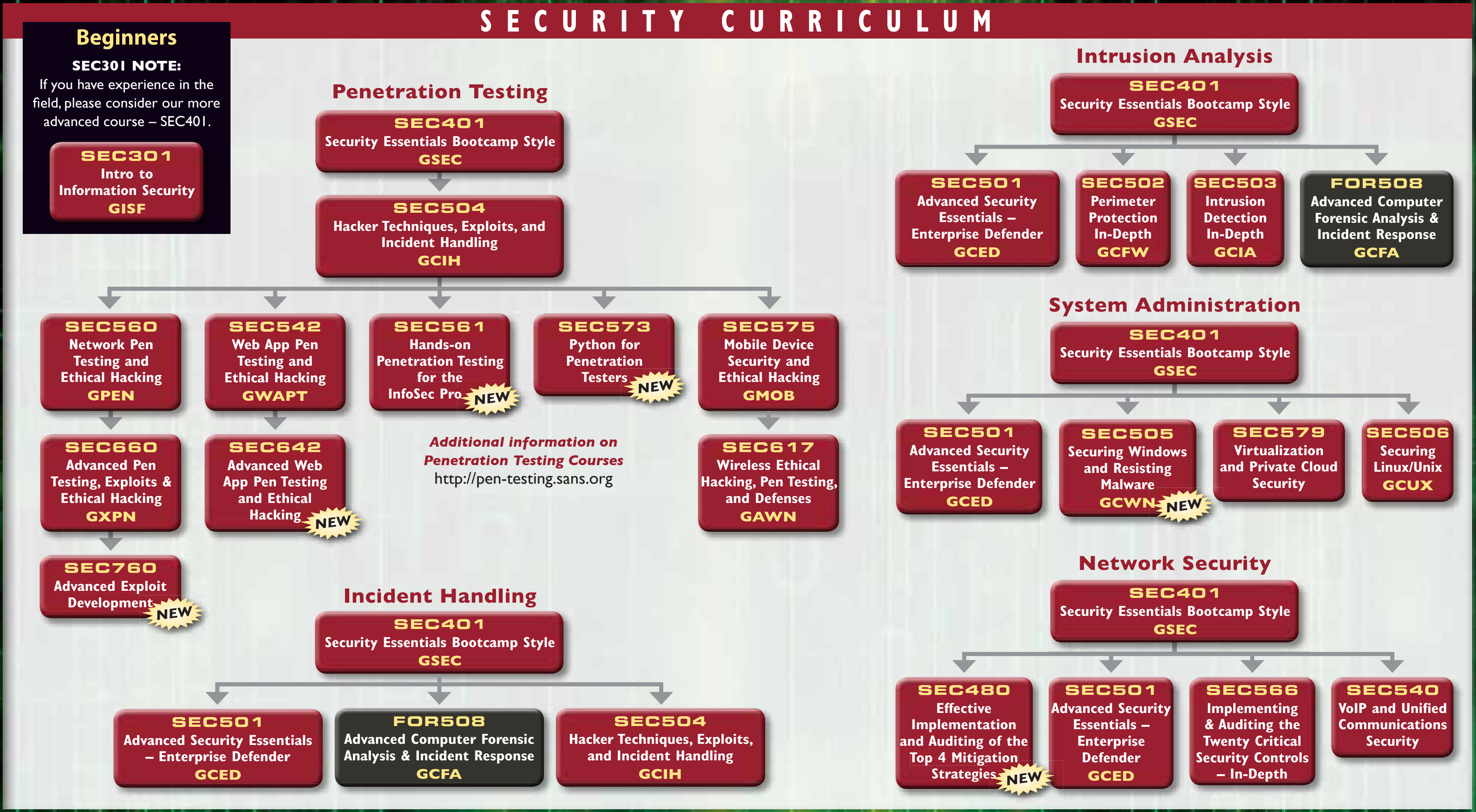
Register at
www.sans.org

Contact us at
AsiaPacific@sans.org

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

GIAC Approved Training

SANS IT Security Training and Your Career Roadmap



SECURITY CURRICULUM

Beginners

SEC301 NOTE:
If you have experience in the field, please consider our more advanced course – SEC401.

SEC301
Intro to Information Security
GISF

Penetration Testing

SEC401
Security Essentials Bootcamp Style
GSEC

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

SEC560
Network Pen Testing and Ethical Hacking
GPEN

SEC542
Web App Pen Testing and Ethical Hacking
GWAPT

SEC561
Hands-on Penetration Testing for the InfoSec Pro
NEW

SEC573
Python for Penetration Testers
NEW

SEC575
Mobile Device Security and Ethical Hacking
GMOB

SEC660
Advanced Pen Testing, Exploits & Ethical Hacking
GXPN

SEC642
Advanced Web App Pen Testing and Ethical Hacking
NEW

SEC617
Wireless Ethical Hacking, Pen Testing, and Defenses
GAWN

SEC760
Advanced Exploit Development
NEW

Additional information on Penetration Testing Courses
http://pen-testing.sans.org

Incident Handling

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

Intrusion Analysis

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

SEC502
Perimeter Protection In-Depth
GCFW

SEC503
Intrusion Detection In-Depth
GCIA

FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA

System Administration

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

SEC505
Securing Windows and Resisting Malware
GCWN
NEW

SEC579
Virtualization and Private Cloud Security

SEC506
Securing Linux/Unix
GCUX

Network Security

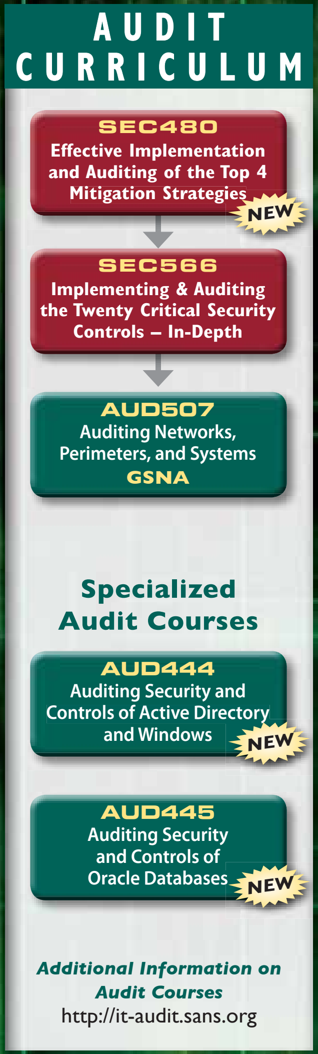
SEC401
Security Essentials Bootcamp Style
GSEC

SEC480
Effective Implementation and Auditing of the Top 4 Mitigation Strategies
NEW

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

SEC566
Implementing & Auditing the Twenty Critical Security Controls – In-Depth

SEC540
VoIP and Unified Communications Security



AUDIT CURRICULUM

SEC480
Effective Implementation and Auditing of the Top 4 Mitigation Strategies
NEW

SEC566
Implementing & Auditing the Twenty Critical Security Controls – In-Depth

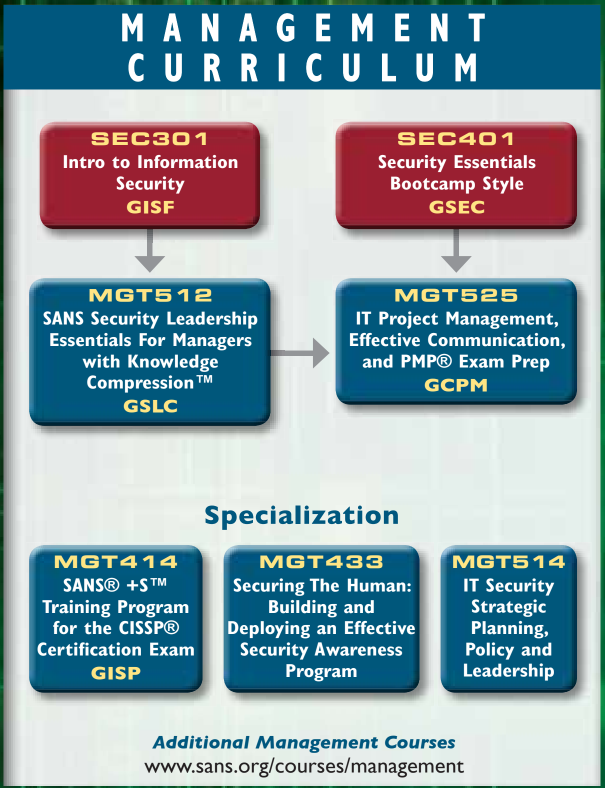
AUD507
Auditing Networks, Perimeters, and Systems
GSNA

Specialized Audit Courses

AUD444
Auditing Security and Controls of Active Directory and Windows
NEW

AUD445
Auditing Security and Controls of Oracle Databases
NEW

Additional Information on Audit Courses
http://it-audit.sans.org



MANAGEMENT CURRICULUM

SEC301
Intro to Information Security
GISF

SEC401
Security Essentials Bootcamp Style
GSEC

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

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

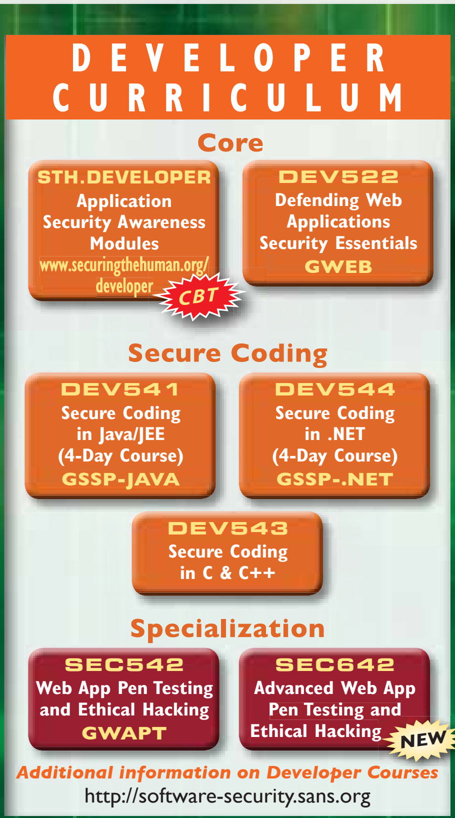
Specialization

MGT414
SANS® +S™ Training Program for the CISSP® Certification Exam
GISP

MGT433
Securing The Human: Building and Deploying an Effective Security Awareness Program

MGT514
IT Security Strategic Planning, Policy and Leadership

Additional Management Courses
www.sans.org/courses/management



DEVELOPER CURRICULUM

Core

STH.DEVELOPER
Application Security Awareness Modules
www.securingthehuman.org/developer
CBT

DEV522
Defending Web Applications Security Essentials
GWEB

Secure Coding

DEV541
Secure Coding in Java/JEE (4-Day Course)
GSSP-JAVA

DEV544
Secure Coding in .NET (4-Day Course)
GSSP-.NET

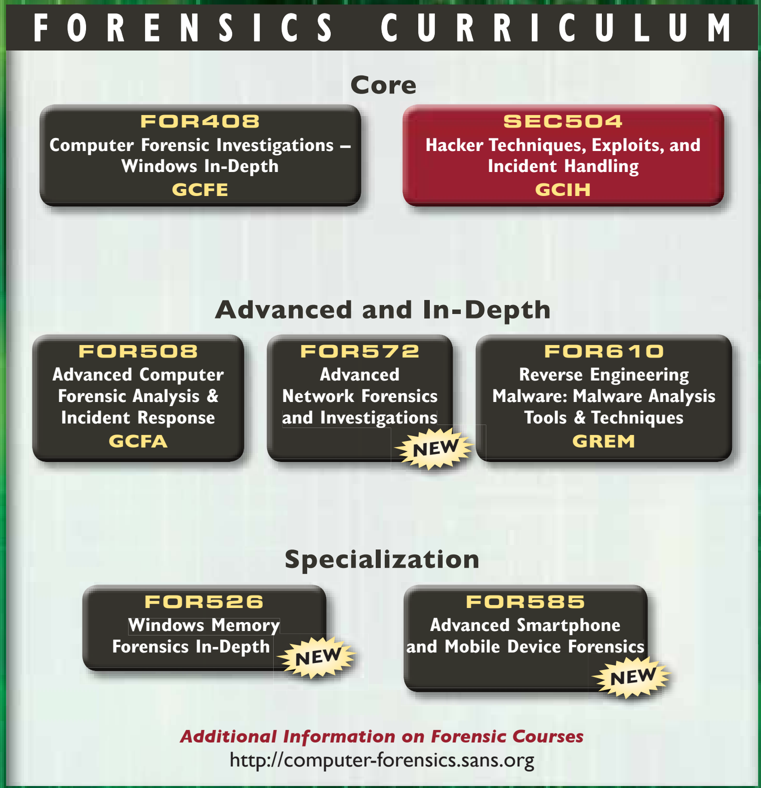
DEV543
Secure Coding in C & C++

Specialization

SEC542
Web App Pen Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Pen Testing and Ethical Hacking
NEW

Additional information on Developer Courses
http://software-security.sans.org



FORENSICS CURRICULUM

Core

FOR408
Computer Forensic Investigations – Windows In-Depth
GCFE

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

Advanced and In-Depth

FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA

FOR572
Advanced Network Forensics and Investigations
NEW

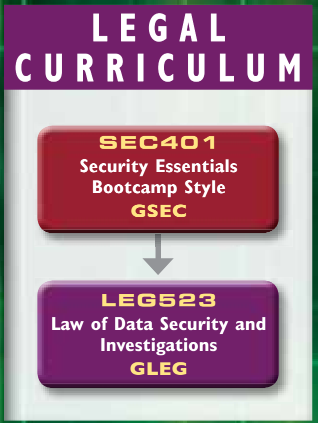
FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

Specialization

FOR526
Windows Memory Forensics In-Depth
NEW

FOR585
Advanced Smartphone and Mobile Device Forensics
NEW

Additional Information on Forensic Courses
http://computer-forensics.sans.org



LEGAL CURRICULUM

SEC401
Security Essentials Bootcamp Style
GSEC

LEG523
Law of Data Security and Investigations
GLEG

GIAC certification available for courses indicated with GIAC acronyms

SANS Asia – Pacific 2014 Event Schedule

Dates and locations may change – for complete up-to-date information, please visit www.sans.org/security-training/bylocation.

	SEC401 Security Essentials Bootcamp Style	SEC480 Effective Implementation and Auditing of the Top 4 Mitigation Strategies NEW!	SEC504 Hacker Techniques, Exploits, and Incident Handling	SEC542 Web App Penetration Testing and Ethical Hacking	SEC560 Network Penetration Testing and Ethical Hacking	SEC575 Mobile Device Security and Ethical Hacking	SEC579 Virtualization and Private Cloud Security	SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking	SEC760 Advanced Exploit Development NEW!	AUD507 Auditing Networks, Perimeters, and Systems	FOR408 Computer Forensic Investigations – Windows In-Depth	FOR508 Advanced Computer Forensic Analysis and Incident Response	FOR526 Windows Memory Forensics In-Depth NEW!	FOR572 Advanced Network Forensics and Investigations NEW!	FOR585 Advanced Smartphone and Mobile Device Forensics NEW!
Secure Canberra Canberra • 12-22 March www.sans.org/event/secure-canberra-2014	SEC401 Page 6	SEC480 Page 7											FOR526 Page 20		
Melbourne Melbourne • 12-17 May www.sans.org/event/melbourne-2014					SEC560 Page 11						FOR408 Page 18				
Canberra Canberra • 30 June - 12 July www.sans.org/event/canberra-2014	SEC401 Week 1 Page 6		SEC504 Week 2 Page 9	SEC542 Week 1 Page 10				SEC660 Week 2 Page 15		AUD507 Week 2 Page 17		FOR508 Week 1 Page 19			FOR585 Week 2 Page 21
Brisbane Brisbane • 1-6 September www.sans.org/event/brisbane-2014					SEC560 Page 11										
Perth Perth • 13-18 October www.sans.org/event/perth-2014	SEC401 Page 6														
Sydney Sydney • 10-22 November www.sans.org/event/sydney-2014	SEC401 Week 1 Page 6	SEC480 Week 2 Page 7	SEC504 Week 2 Page 9			SEC575 Week 1 Page 13	SEC579 Week 2 Page 14		SEC760 Week 1 Page 16					FOR572 Week 2 Page 21	

	SEC401 Security Essentials Bootcamp Style	SEC480 Effective Implementation and Auditing of the Top 4 Mitigation Strategies NEW!	SEC503 Intrusion Detection In-Depth	SEC504 Hacker Techniques, Exploits, and Incident Handling	SEC542 Web App Penetration Testing and Ethical Hacking	SEC546 IPv6 Essentials	SEC560 Network Penetration Testing and Ethical Hacking	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking	FOR408 Computer Forensic Investigations – Windows In-Depth	FOR508 Advanced Computer Forensic Analysis and Incident Response	FOR526 Windows Memory Forensics In-Depth NEW!	FOR559 Cloud Forensics & Incident Response NEW!	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Secure Singapore Singapore • 10-26 March www.sans.org/event/secure-singapore-2014		SEC480 Page 7		SEC504 Page 9	SEC542 Page 10				SEC660 Page 15	FOR408 Page 18			FOR559 Page 21	FOR610 Page 22
October Singapore Singapore • 13-18 October www.sans.org/event/october-singapore-2014	SEC401 Page 6		SEC503 Page 8			SEC546 Page 23	SEC560 Page 11	SEC575 Page 13			FOR508 Page 19	FOR526 Page 20		

SANS Asia – Pacific 2014 Event Schedule

Dates and locations may change – for complete up-to-date information, please visit www.sans.org/security-training/bylocation.

	SEC401 Security Essentials Bootcamp Style	SEC503 Intrusion Detection In-Depth	SEC504 Hacker Techniques, Exploits, and Incident Handling	SEC542 Web App Penetration Testing and Ethical Hacking	SEC560 Network Penetration Testing and Ethical Hacking	SEC575 Mobile Device Security and Ethical Hacking	SEC579 Virtualization and Private Cloud Security	SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking	FOR508 Advanced Computer Forensic Analysis and Incident Response	FOR526 Windows Memory Forensics In-Depth NEW!	FOR572 Advanced Network Forensics and Investigations NEW!
Secure India @ Bangalore Bangalore • 17-22 February www.sans.org/event/secure-india-2014			SEC504 *Page 9*	SEC542 *Page 10*		SEC575 *Page 13*			FOR508 *Page 19*		
Delhi Delhi • 9-14 June www.sans.org/event/delhi-2014							SEC579 *Page 14*			FOR526 *Page 20*	
Bangalore Bangalore • 22-27 September www.sans.org/event/bangalore-2014	SEC401 *Page 6*	SEC503 *Page 8*						SEC660 *Page 15*			FOR572 *Page 21*
Hyderabad/Chennai Hyderabad/Chennai • 24-29 November www.sans.org					SEC560 *Page 11*						

	FOR408 Computer Forensic Investigations – Windows In-Depth
Indonesia Jakarta • 7-12 April www.sans.org/event/indonesia-2014	FOR408 *Page 18*

	SEC560 Network Penetration Testing and Ethical Hacking	FOR508 Advanced Computer Forensic Analysis and Incident Response
Malaysia @ MCMC Cyberjaya • 19-24 May www.sans.org/event/malaysia-2014	SEC560 *Page 11*	FOR508 *Page 19*

	SEC542 Web App Penetration Testing and Ethical Hacking	SEC561 Hands-on Penetration Testing for the InfoSec Pro NEW!	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Tokyo Autumn Tokyo • 10-15 November www.sans.org/event/tokyo-autumn-2014	SEC542 *Page 10*	SEC561 *Page 12*	FOR610 *Page 22*

	SEC401 Security Essentials Bootcamp Style	SEC504 Hacker Techniques, Exploits, and Incident Handling	SEC560 Network Penetration Testing and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking
Secure Thailand Bangkok • 26-31 May www.sans.org/event/secure-thailand-2014	SEC401 *Page 6*		SEC560 *Page 11*	
Bangkok Bangkok • 18-30 August www.sans.org/event/bangkok-2014		SEC504 *Page 9*		SEC660 *Page 15*

	SEC504 Hacker Techniques, Exploits, and Incident Handling	SEC560 Network Penetration Testing and Ethical Hacking	SEC575 Mobile Device Security and Ethical Hacking	FOR508 Advanced Computer Forensic Analysis and Incident Response	FOR585 Advanced Smartphone and Mobile Device Forensics NEW!
Cyber Defense Korea Seoul • 9-14 June www.sans.org/event/cyber-defense-korea-2014		SEC560 *Page 11*	SEC575 *Page 13*		
Seoul Seoul • 10-15 November www.sans.org/event/seoul-2014	SEC504 *Page 9*			FOR508 *Page 19*	FOR585 *Page 21*

SECURITY 401

Six-Day Program | Laptop Required | 46 CPE/CMU Credits | GIAC Cert: GSEC

SEC401: Security Essentials Bootcamp Style

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but on the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems. SEC401 Security Essentials teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In additional to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

> *"I'm a newbie to security. This course presented a ton of information on this subject in a fast-paced, easy-to-understand manner."*
>
> -Michael Horkan,
> Rockwell Automation

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

1. What is the risk?

2. Is it the highest priority risk?

3. Is it the most cost-effective way of reducing the risk?

> *"The course provides fundamental understanding of 'Defense In-Depth' strategies and capabilities."*
>
> -Alan Turney,
> Department of Defence

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

www.giac.org

DoD 8570 Required
www.sans.org/8570

www.sans.org/
cyber-guardian

www.sans.edu

Who Should Attend

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

You Will Be Able To

- Design and build a network architecture using VLAN's, NAC and 802.1x based on APT indicator of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and determine a checklist that can be used to validate the security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilizing various tools to include dumpsec and OpenVAS - and once vulnerabilities are discovered cover ways to configure the system to be more secure
- Determine overall scores for systems utilizing CIS Scoring Tools and create a system baseline across the organization
- Build a network visibility map that can be used for hardening of a network - validating the attack surface and covering ways to reduce the attack surface through hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords and vulnerabilities utilizing WireShark

SEC480: Effective Implementation and Auditing of the Top 4 Mitigation Strategies

Over the past three years, there has been an ever-increasing focus on preventing targeted cyber intrusions around the world. The Australian Defence Signals Directorate (DSD) responded to the sharp increase in intrusion activity with the 'Strategies to Mitigate Targeted Cyber Intrusions'. This is a list of 35 strategies that organizations can implement to reduce the likelihood of a successful cyber intrusion.

DSD has since stated that implementing even just the top 4 of these strategies would have successfully prevented over 85% of the incidents the organization currently responds to. Based on the effectiveness of these strategies, the Australian Government declared that the Top 4 strategies are now mandatory for all Australian Government agencies, these strategies are:

1. **Application Whitelisting**
2. **Patch Applications**
3. **Patch Operating Systems**
4. **Minimize Administrative Privileges**

This course will provide students the skills necessary to implement these strategies in their organizations and environments. The course will cover the following:

- **The techniques used in targeted cyber intrusions**
- **The importance of the Top 4, including their effectiveness**
- **Practical demonstrations of these technologies in action, including hands-on labs**
- **Implementation strategies and communication methods**
- **Use of these strategies to detect and prevent unknown threats/advanced persistent threats**

After attending this hands-on course, individuals will be able to effectively and successfully implement these strategies to detect and prevent targeted cyber intrusions.

Who Should Attend

- General security practitioners
- Network engineers
- System, security, and network administrators
- System administrators who are on the front-lines defending their systems and responding to attacks
- Hands-on security managers

You Will Be Able To

- Plan and implement an effective Application Whitelisting solution
- Gain hands on experience with a number of Application Whitelisting technologies
- Understand and overcome current limitations and business challenges of Application Whitelisting
- Design business processes and implement solutions to support rapid and reliable patch deployments
- Effectively minimize administrative privileges in enterprise environments
- Audit Top 4 Mitigation Strategy implementations to ensure they are providing a high level of security and assurance

SEC503: Intrusion Detection In-Depth

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

> *"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."*
>
> -Thomas Kelly, DIA

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

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

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

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

Who Should Attend

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

You Will Be Able To

- Identify the security solutions that are most important for protecting your perimeter
- Understand attacks that affect security for the network
- Understand the complexities of IP and how to identify malicious packets
- Understand the risks and impacts related to Cloud Computing and security solutions to manage the risks
- Understand the process for properly securing your perimeter
- Identify and understand how to protect against application and database risks
- Use tools to evaluate the packets on your network and identify legitimate and illegitimate traffic

> *"Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts."*
>
> -Hector Araiza, USAF

www.giac.org

DoD 8570 Required
www.sans.org/8570

www.sans.org/
cyber-guardian

www.sans.edu

SECURITY 504

Six-Day Program | Laptop Required | 37 CPE/CMU Credits | GIAC Cert: GCIH

SEC504: Hacker Techniques, Exploits, and Incident Handling

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

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

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

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

> ***"This class teaches you all of the hacking techniques that you need as an incident handler."***
>
> -Demonique Lewis, TerpSys

www.giac.org

DoD 8570 Required
www.sans.org/8570

www.sans.org/cyber-guardian

www.sans.edu

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

You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques to be able to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access of a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
- Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques and choosing appropriate response actions based on each attacker's flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

SECURITY 542

Six-Day Program | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GWAPT

SEC542: Web App Penetration Testing and Ethical Hacking

Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate to advanced level class, you'll learn the art of exploiting web applications so you can find flaws in your enterprise's web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

> *"Without a doubt, this was the best class for my career."*
> -Don Brown, Lockheed Martin

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's web applications to find some of the most common and damaging Web application vulnerabilities today.

> *"Fun while you learn! Just don't tell your manager. Every class gives you invaluable information from real world testing you cannot find in a book."*
> -David Fava, The Boeing Company

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

www.giac.org

DoD 8570 Required
www.sans.org/8570

www.sans.org/
cyber-guardian

www.sans.edu

Who Should Attend

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

You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests, including Recon, Mapping, Discovery, and Exploitation
- Analyze the results from automated web testing tools to remove false positives and validate findings
- Use python to create testing and exploitation scripts during a penetration test
- Create configurations and test payloads within Burp Intruder to perform SQL injection, XSS, and other web attacks
- Use FuzzDB to generate attack traffic to find flaws such as Command Injection and File Include issues
- Assess the logic and transaction flaw within a target application to find logic flaws and business vulnerabilities
- Use the rerelease of Durzosploit to obfuscate XSS payloads to bypass WAFs and application filtering
- Analyze traffic between the client and the server application using tools such as Ratproxy and Zed Attack Proxy to find security issues within the client-side application code
- Use BeEF to hook victim browsers, attack the client software and network, and evaluate the potential impact XSS flaws have within an application
- Perform a complete web penetration test during the Capture the Flag exercise to pull all of the techniques and tools together into a comprehensive test

> ***"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."***
> -Brad Milhorn, ii2P LLC

SECURITY 560

Six-Day Program | Laptop Required | 37 CPE/CMU Credits | GIAC Cert: GPEN

SEC560: Network Penetration Testing and Ethical Hacking

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. SANS SEC560: Network Penetration Testing and Ethical Hacking truly prepares you to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course.

> *"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend."*
>
> -Mark Hamilton, McAfee

Equipping Security Organizations with Advanced Penetration Testing and Ethical Hacking Know-How

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then, we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective. The final portion of the class includes a comprehensive hands-on exercise, conducting a penetration test against a hypothetical target organization, following all of the steps.

> *"The skills taught and demonstrated in this class are perfect for new pen testers and veterans alike."*
>
> -Roy Luongo, Dept of Defense

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

www.giac.org

www.sans.org/cyber-guardian

www.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

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Configure and launch a vulnerability scanner such as Nessus so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
- Utilize the Windows and Linux command lines to plunder target systems for vital information that can further the overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
- Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks
- Utilize wireless attacks tools for Wifi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys, and exploit client machines included within a project's scope
- Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL Injection vulnerabilities to determine the business risk faced by an organization

SEC561: Hands-on Penetration Testing for the InfoSec Pro

Today, many information security practitioners are expected to leverage cross-disciplinary skills in complex areas. Analysts are no longer able to specialize in just a single skill area, such as vulnerability assessment, network penetration testing, or web app assessment. To face todays threats, organizations need employees that add value to the team across varying focus areas, contributing to both operations and security teams.

Few practitioners have the time to build broad skills across many different security areas. The best way to pick up new skills quickly is to practice them in hands-on, real-world scenarios designed to challenge and guide a participant. The Hands-On Security Practitioner course creates a learning environment where participants can quickly build and reinforce skills in multiple focus areas, including:

- **Network security assessment, identifying architecture weaknesses in network deployments**
- **Host-based security assessment, protecting against privilege escalation attacks**
- **Web application penetration testing, exploiting common flaws in complex systems**
- **Advanced system attacks, leveraging pivoting and tunneling techniques to identify exposure areas deep within an organization**

The Hands-On Security Practitioner course departs from most lecture-based training models to help practitioners quickly build skills in many different information security focus areas. Using the NetWars challenge platform, participants engage in practical and real-world defensive and offensive Capture the Flag (CtF) exercises that are fun and exciting. By maximizing hands-on time in exercises, participants build valuable skills that are directly applicable as soon as they return to the office.

Participants who complete the Hands-On Security Practitioner participate in realistic scenarios to quickly build skills that are difficult to achieve independently. After completing the course, participants will be able to apply these skills to various areas within their own organizations, significantly increasing their ability to take on cross-disciplinary projects and tasks.

Who Should Attend

- Security professionals that 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 that 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 analysis through experience with real-world attacks
- Penetration testers seeking to gain practical hands-on experience for use in their own assessments

You Will Be Able To

- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorized server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulating common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common web application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- Harvest sensitive mobile device data from iOS and Android targets

SECURITY 575

Six-Day Program | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GMOB

SEC575: Mobile Device Security and Ethical Hacking

Now updated to cover Apple iOS 6, BlackBerry 10, Android Jelly Bean, and Windows Phone 8

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 email access as well as 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 enterprise resource planning 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.

> ***"Wow! This course is everything you need to know about mobile device deployment, risks and more. Don't deploy your mobile devices without taking this course first."***
>
> -Bryan Simon, INTEGRIS Credit Union

The security risks of mobile phone and tablet device use in the workplace

Whether the device is an Apple iPhone or iPad, a Windows Phone, 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.

From mobile device security policy development, to design and deployment, and more

> ***"With the mad rush towards mobile device adoption at the point of sale and industry regulations and laws struggling to keep up, thank goodness SANS helps companies maintain secure operations."***
>
> -Dean Altman, Discount Tire

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 practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, 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 from 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.

Who Should Attend

- Security personnel whose job involves assessing, deploying, or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills

You Will Be Able To

- Develop effective policies to control employee-owned (Bring Your Own Device, BYOD) and enterprise-owned mobile devices including the enforcement of effective passcode policies and permitted application
- Utilize jailbreak tools for Apple iOS and Android systems such as redsn0w and Absinthe
- Conduct an analysis of iOS and Android filesystem data using SqliteSpy, Plist Editor, and AXMLPrinter to plunder compromised devices and extract sensitive mobile device use information such as the SMS history, browser history, GPS history, and user dictionary keywords
- Analyze Apple iOS and Android applications with reverse engineering tools including class-dump, JD-GUI, dex-translator, and apktool to identify malware and information leakage threats in mobile applications
- Conduct an automated security assessment of mobile applications using iAuditor, Cycript, MobileSubstrate, TaintDroid, and DroidBox to identify security flaws in mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks, crack WEP and WPA/WPA2 access points, bypass enterprise wireless network authentication requirements, and harvest user credentials
- Intercept and manipulate mobile device network activity using Burp to manipulate the actions taken by a user in an application and to deliver mobile device exploits to vulnerable devices

www.giac.org www.sans.edu

SEC579: Virtualization and Private Cloud Security

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.

> *"Eye-opening class taught by an engaging and highly knowledgeable industry leader."*
> -Sanford Walke, Holcim US, Inc.

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.

The class starts out with two days of architecture and security design for both virtualization and private cloud infrastructure. The entire gamut of components will be covered ranging from hypervisor platforms to virtual networking, storage security to locking down the individual virtual machine files. We'll describe how to secure the management interfaces and servers, delve into Virtual Desktop Infrastructure (VDI), and go in-depth on what to consider when building a private cloud from existing virtualization architecture. Finally, we'll look at integrating virtual firewalls and intrusion detection systems into the new architecture for access control and network monitoring.

The next two days we'll go into detail on offense and defense - how can we assess virtualized environment using scanning and pen testing tools and techniques, and how do things change when we move to a cloud model? We'll cover a variety of scanners and vulnerability management tools and practices, and then take a hard look at virtualization vulnerabilities, exploits, and toolkits for pen testing that we can put to use in class.

Once we cover the offense, we'll take the opposite approach and go into detail on performing intrusion detection and logging within the virtual environment, as well as covering anti-malware advances and changes within virtual infrastructure. We'll wrap up the session with coverage of incident handling within virtual and cloud environments, as well as adapting forensics processes and tools to ensure we can maintain chain-of-custody and perform detailed analysis of virtualized assets.

> *"I plan to (eventually) send everyone in my Net Ops and Cyber Security shops to this course. It seems indispensable."*
> -Keil Hubert, 136th Comm. Flight

During day 5, we will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. We'll show you how to design a foundational risk assessment program and then build on this with policies, governance, and compliance considerations within your environment. We'll cover auditing and assessment of your virtualized assets, with a session on scripting that will help you put this into practice right away. Then we'll go in-depth into data security within a private cloud environment, discussing encryption and data lifecycle management techniques that will help you keep up with data that are much more mobile than ever before. Identity and Access Management (IAM) within a virtualized/cloud environment will be touched on, and we'll wrap up with a thorough session on disaster recovery and business continuity planning that leverages and benefits from virtualization and cloud-based technology.

On day 6, we'll cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most important and critical things to take away from these to implement. We culminate with data security and encryption, and Identity and Access Management (IAM) and Disaster Recovery (DR) and Business Continuity Planning (BCP).

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

You Will Be Able To

- Lock down and maintain a secure configuration for all components of a virtualization environment
- Design a secure virtual network architecture
- Evaluate virtual firewalls, intrusion detection and prevention systems, and other security infrastructure
- Evaluate security for private cloud environments
- Perform vulnerability assessments and pen tests in virtual and private cloud environments, and acquire forensic evidence
- Perform audits and risk assessments within a virtual or private cloud environment

SECURITY 660

Six-Day Program | Laptop Required | 46 CPE/CMU Credits | GIAC Cert: GXPN

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking

This course is designed as a logical progression point for those who have completed SANS SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, Return Oriented Programming (ROP), Windows exploit-writing, and much more!

> ***"This course is an excellent tour into the advanced skills needed for current/effective penetration."***
>
> -Matthew Smith, U.S. Dept. of Homeland Security

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, one must have a strong desire to learn, the support of others, and the opportunity to practice and build experience. SANS SEC660 engages attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing advanced penetration concepts, and an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using Return Oriented Programming (ROP) and other techniques. Local and remote exploits, as well as client-side exploitation techniques are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

> ***"Most comprehensive coverage of fuzzing. I would have signed up for the course for that alone."***
>
> -Adam Kliarsky, Cedars-Sinai Medical Center

www.giac.org

www.sans.org/cyber-guardian

www.sans.edu

Who Should Attend

- Network and Systems Penetration Testers
- Incident Handlers
- Application Developers
- IDS Engineers

You Will Be Able To

- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse engineer vulnerable code to write custom exploits

> ***"The breadth and depth of information that this course covers in spectacular detail shines with the glory of a thousand suns."***
>
> -Jacob Horne, Department of Defense

Six-Day Program | Laptop Required | 36 CPE/CMU Credits

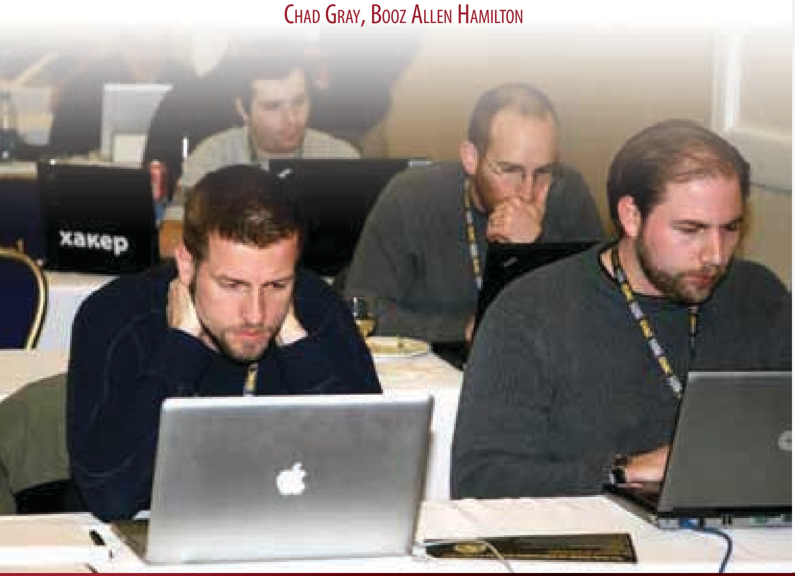
SEC760: Advanced Exploit Development for Penetration Testers

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet, they could expose organizations to significant attacks, undermining their defenses when wielded by very skilled attackers. Few security professionals have the skillset to discover, let alone even understand at a fundamental level, why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SANS SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse engineer 32-bit and 64-bit applications, perform remote-user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploits against modern software and operating systems.

"SANS training teaches what it takes to do your job right."
-Jeff Turner, Lexis Nexis

As a prerequisite, students are expected to know how to use debuggers such as GDB and Immunity Debugger, as well as techniques such as how to quickly build a ROP chain to disable DEP and bypass ASLR as part of an exploit. Remedial stack overflows and basic techniques to evade exploit mitigation controls are assumed knowledge, as well as experience with programming languages such as C, C++, and Python. Development experience is not required, but experience with disassembling x86 binaries is required. The skills taught in the SANS SEC660 course on Advanced Penetration Testing, Exploits, and Ethical Hacking are a helpful background for preparing for this 760 course.

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



Who Should Attend

- Senior network and system penetration testers
- Secure application developers – (C & C++)
- Reverse-engineering professionals
- Vulnerability researchers
- Security researchers

You Will Be Able To

- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- Perform remote debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows
- Write Return Oriented Shellcode
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows heap overflows and use-after-free attacks
- Use precision heap sprays to improve exploitability
- Perform Windows Kernel debugging up through Windows 8 64-bit
- Windows Kernel exploitation

AUDIT 507

Six-Day Program | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GSNA

AUD507: Auditing Networks, Perimeters, and Systems

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

> *"This course is full of relevant, timely, current content, delivered in a highly engaging style. This course is a must for IT auditors and security specialists."*
>
> -Brooks Adams,
> Georgia Southern University

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

> *"This course is full of relevant, timely, current content, delivered in a highly engaging style. This course is a must for IT auditors and security specialists."*
>
> -Brooks Adams,
> Georgia Southern University

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

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

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and experience the mix of theoretical, hands-on, and practical knowledge.

Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

You Will Be Able To

Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit

- Conduct a proper network risk assessment to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks—a standard to conduct an audit against
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources.
- Audit web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

GSNA

www.giac.org

DoD 8570 Required
www.sans.org/8570

SANS INSTITUTE
www.sans.edu

FORENSICS 408

Six-Day Program | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GCFE

FOR408: Computer Forensic Investigations – Windows In-Depth

> *"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."*
> -Alexander Applegate, Auburn University

Master Windows Forensics. Learn Critical Analysis Techniques.

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 agencies also need the skills to perform media exploitation and recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together what happened.

FOR408: Computer Forensic Investigations – Windows In-Depth focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation.

This course covers the methodology of in-depth computer forensic examinations, digital investigative analysis, and media exploitation so each student will have complete qualifications to work as a computer forensic investigator helping to solve and fight crime. In addition to in-depth technical knowledge of Windows Digital Forensics (Windows XP through Windows 8 and Server 2012), you will learn about well-known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that students can take with them.

What you will receive with this course

- **Windows version of the SIFT Workstation Virtual Machine**
- **Windows 8 Standard Full Version License and Key for the Windows SIFT Workstation**
- **Full License to AccessData FTK and Guidance Software EnCase for a 3 month trial**
- **Full License to MagnetForensics Internet Evidence Finder for a 15 day trial**
- **Two full real-world cases to examine during class**
- **Course DVD loaded with case examples, tools, and documentation**
- **Wiebetech Ultradock v5 Write Blocker Kit**

www.giac.org

www.sans.edu

Digital Forensics and Incident Response
http://computer-forensics.sans.org

Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

You Will Be Able To

- Perform proper Windows forensic analysis, determine who placed an artifact on the system and how they did it by applying key analysis techniques covering Windows XP through Windows 8
- Use full-scale forensic tools and analysis methods to detail every action a suspect accomplished on a Windows system – and determine program execution, file/folder opening, geo-location, browser history, USB devices, and more
- Uncover the exact time that a specific user last executed a program through Registry analysis, Windows artifact analysis, and email analysis. Over time that is key to proving intent in many cases such as intellectual property theft, hacker breached systems, and traditional crimes
- Demonstrate every time a file has been opened by a suspect through IE browser forensics, shortcut file analysis (LNK), email analysis and Registry parsing • Use automated analysis techniques via AccessData's Forensic ToolKit (FTK)
- Identify key words searched for by a specific user on a Windows system that can be used to identify files that the suspect was interested in finding
- Use shellbags analysis tools to articulate every folder and directory that a user opened up while he was browsing through the hard drive
- Determine each time a unique and specific USB device is attached to the Windows system, the files and folders that were accessed on it, and who plugged it in via tools parsing key Windows artifacts such as the Registry and log files
- Examine how a user logged into a Windows system through a remote session, at the keyboard, or simply unlocking their screensaver by viewing the logon types in the Windows security event logs
- Use FTK Registry Viewer, pinpoint geo-location of a Windows system through the examination of the networks they have connected to, browser search terms, and cookie data to determine where a crime was committed
- Use Web Historian, recover browser history of a suspect who has attempted to clear their trail using in-private browsing through the recovery of session restore points and flash cookies

FORENSICS 508

Six-Day Program | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GCFA

FOR508: Advanced Computer Forensic Analysis and Incident Response

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

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

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

> *"The SANS FOR508 course exceeded my expectations in every way. It provided me the skills, knowledge, and tools to effectively respond to and handle apts and other enterprise-wide threats."*
>
> -Josh Moulin, NSTEC/NNSA/DOE

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

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

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

What you will receive with this course

- **SIFT Workstation Virtual Machine**
- **F-Response TACTICAL Edition with a 2 year license**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **64 GB SANS DFIR USB Key loaded to the brim with Windows XP, Win7, Win2008R2 live response data, memory images, and full system hard drive images of a compromised enterprise network**
- **Course DVD loaded with case examples, additional tools, and documentation**

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

www.giac.org

www.sans.edu

Digital Forensics and Incident Response
http://computer-forensics.sans.org

Who Should Attend

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

You Will Be Able To

- Apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments from Advanced Persistent Threat (APT) groups, organized crime syndicates, or hackivists
- Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- Use the SIFT Workstation's capabilities, perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first, allowing for immediate response and scalable analysis to take place across the enterprise
- Use system memory and the Volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response
- Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI) to quickly ascertain the threat to your organization and aid in scoping the true extent of the data breach
- Track the exact footprints of an attacker crossing multiple systems and observe data they have collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS $I30 directory file indexes, journal parsing, and detailed Master File Table analysis
- Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- Discover an adversary's persistence mechanisms to allow malware to continue to run on a system after a reboot using command-line tools such as autorunsc, psexec, jobparser, group policy, triage-ir, and IOCFinder

FOR526: Windows Memory Forensics In-Depth

FOR526 - Memory Analysis In-Depth is a critical course for any serious investigator who wishes to tackle advanced forensic and incident response cases. Memory analysis is now a crucial skill for any investigator who is analyzing intrusions.

> *"The presentation, exercises, labs, and data provided are the best in the computer forensics industry."*
>
> -Rebecca Passmore, FBI

Malware can hide, but it must run – the malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis. Learn how memory analysis works by learning about memory structures and context, memory analysis methods, and the current tools used to parse system ram.

Attackers will use anti-forensic techniques to hide their tracks. They use rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware to hide in plain sight avoiding detection by standard host-based security measures. Every action that adversaries make will leave a trace; you merely need to know where to look. Memory analysis will give you the edge that you need in order to discover advanced adversaries in your network.

> *"This is the best SANS course I have taken so far with the best instructor. I hope to take more classes in the future."*
>
> -Jonathan Hinson, Duke Energy

FOR526 - Memory Analysis In-Depth is one of the most advanced courses in the SANS Digital Forensics and Incident Response Curriculum. This cutting-edge course covers everything you need to step through memory analysis like a pro.

> *"Totally awesome, relevant and eye opening. I want to learn more every day."*
>
> -Matthew Britton, Blue Cross Blue Shield of Louisiana

Digital Forensics and Incident Response
http://computer-forensics.sans.org

Who Should Attend

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- And anybody who plays a part in the acquisition, preservation,forensics, or analysis of Microsoft Windows computers.

You Will Be Able To

- Utilize stream-based data parsing tools to extract AES-encryption keys from a physical memory image to aid in the decryption of encryption files & volumes such as TrueCrypt & BitLocker
- Gain insight into the current network activity of the host system by retrieving network packets from a physical memory image and examining it with a network packet analyzer
- Inspect a Windows crash dump to discern processes, process objects and current system state at the time of crash through use of various debugging tools such as kd,WinDBG, and livekd
- Conduct Live System Memory Analysis with the powerful SysInternal's tool, Process Explorer, to collect real-time data on running processes allowing for rapid triage
- Use the SIFT workstation and in-depth knowledge of PE File modules in physical memory, extract and analyze packed and non-packed PE binaries from memory and compare them to their known disk-bound files
- Discover key features from memory such as the BIOS keyboard buffer, Kernel Debugging Data Block (KDBG), Executive Process (EPROCESS) structures, and handles based on signature and offset searching, gaining a deeper understanding of the inner workings of popular memory analysis tools
- Analyze memory structures using high-level and low-level techniques to reveal hidden and terminated processes and extract processes, drivers, and memory sections for further analysis
- Use a variety of means to capture memory images in the field, explaining the advantages and limitations of each method

NEW!

FORENSICS 559

Six-Day Program | Laptop Required | 36 CPE/CMU Credits

FOR559: Cloud Forensics & Incident Response

This course will focus on both the collection of evidence in a sound manner from a Private and Public Cloud environment for external analysis as well as performing the complete evidence collection, IR and Forensics Analysis "within" a Private and Public Cloud environment (all work is performed within the Cloud).

Course Topics:

- Forensics In "End-user / Retail" Cloud Storage
- Cloud Forensics Challenges – Incident Response Perspective
- IR & Forensics - VMware & HyperV Private Clouds
- Cloud Forensics Organizational Structure
- SLA Considerations
- Cloud Models – IAAS, PAAS, SAAS
- Key Issues In Cloud Forensics
- Cloud IR & Forensics – Amazon, Azure, OpenStack and RackSpace
- Cloud Forensics Challenge

NEW!

FORENSICS 572

Six-Day Program | Laptop Required | 36 CPE/CMU Credits

FOR572: Advanced Network Forensics and Analysis

The network is a common domain for almost all modern attacks. Even if a savvy attacker effectively hides their tracks on a compromised system, or the system has long been wiped, the network evidence remains - and is usually more than needed to conduct a thorough investigation. This course will teach students to follow an attacker's footprints and analyze evidence from a networked environment. During hands on exercises, you will use tools such as tcpdump, Wireshark, Snort, and tcpxtract. You'll analyze netflow data, logging servers, as well as pcap files to understand the attacks and reconstruct the incident without ever using an endpoint's hard drive. Students will build and use skills from across the forensic and investigative domains using a modified Linux SIFT Workstation VM.

Course Topics:

- Carve files from packet capture
- Wireless networking
- tcpdump and wireshark hands-on
- Network architectural challenges and opportunities
- HTTPS / SSL Inspection
- Netflow analysis
- Visualization tools and techniques
- Log data collection, aggregation and analysis
- Encrypted traffic flow analysis (SSL, IPSEC, PPTP, etc)
- Automated tool exercises

NEW!

FORENSICS 585

Six-Day Program | Laptop Required | 36 CPE/CMU Credits

FOR585: Advanced Smartphone & Mobile Device Forensics

Since smartphones and other mobile devices can contain details about who was doing what, where and when, their usefulness as a source of information in any investigation should never be underestimated.

This course focuses on smartphones as sources of evidence, providing forensic practitioners, incident responders, and computer security professionals with the necessary skills to handle smartphones and other mobile devices in a forensically sound manner, to acquire and examine digital evidence from these devices, and to analyze the results for use in digital investigations. Students will be able to recover and analyze data for use in internal investigations, criminal and civil litigation, investigation and resolution of security breaches, and to obtain actionable intelligence. FOR585 addresses today's smartphone technologies and threats by providing real-life, hands-on investigative scenarios.

FORENSICS 610

Six-Day Program | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GREM

FOR610: Reverse-Engineering Malware: Malware Analysis Tools & Techniques

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs—spyware, bots, trojans, etc.—that target or run on Microsoft Windows. This training also looks at reversing web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

> *"This class gave me essential tools that I can immediately apply to protect my organization."*
> -Don Lopez, Valley National Bank

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

The course begins by covering fundamental aspects of malware analysis. The course continues by discussing essential x86 assembly language concepts. Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents.

> *"I thought I knew reversing. This class taught me so much more and provided easy understandings of complex reversing tasks."*
> -David Werden, NGIS

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware.

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss malware analysis tools and techniques of intermediate complexity. Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops, and functions. The course spends some time discussing essential aspects of x86 assembly to allow malware analysts to navigate through malicious executables using a debugger and a disassembler.

> *"Highly valuable content, greatly increased my understanding of malware and techniques to reverse engineer."*
> -Kenneth Miltenberger, US Coast Guard

www.giac.org

www.sans.edu

Digital Forensics and Incident Response
http://computer-forensics.sans.org

Who Should Attend

- Professionals with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration
- Professionals who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs
- Individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their malware forensics expertise

You Will Be Able To

- Build an isolated laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes on Microsoft Windows
- Uncover and analyze malicious JavaScript, VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- Control some aspect of the malicious program's behavior through network traffic interception and code patching
- Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files in the context of targeted attacks
- Derive Indicators of Compromise (IOCs) from malicious executables to contain and recover from the incident
- Utilize practical memory forensics techniques to examine capabilities of rootkits

SKILL-BASED SHORT COURSE

SECURITY 546

Two-Day Course | Laptop Required | 12 CPE/CMU Credits

SEC546: IPv6 Essentials

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 over the next years to grow, in particular as mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats unintentional IPv6 use may bring.

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more and more important to global commerce.

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

This course will introduce network administrators and security professionals to the basic concepts of IPv6. While it is an introduction to IPv6, it is not an introduction to networking concepts. You should understand and be aware of the basic concepts of IPv4, and networking in general. It is an ideal refresher if you took SEC503 Intrusion Detection in Depth. However, you do not need to know IPv4 in the full detail in which it is presented in SEC503. The networking and IPv4 principles taught in SEC401 Security Essentials should prepare you for this course.

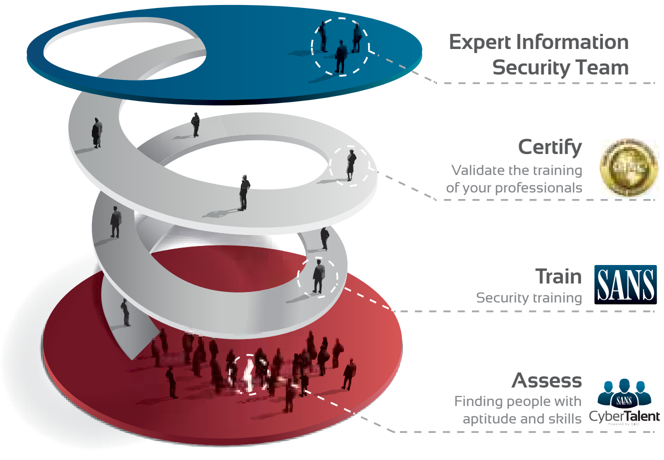
SANS CyberTalent Powered by GIAC

Contact Us to Learn More

www.sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

Introducing SANS CyberTalent Assessments, a new web-based recruitment and talent management tool that helps validate the skills of information security professionals. This unique tool may be used during the recruitment process of new information security employees and to assess the skills of your current staff to create a professional development plan. This tool will save you money and time, as well as provide you with the information required to ensure you have the right skills on your information security team.



Expert Information Security Team
Certify
Validate the training of your professionals
Train
Security training
SANS
Assess
Finding people with aptitude and skills
CyberTalent

Benefits of SANS CyberTalent Assessments

For Recruiting

- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

For Talent Management

- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps develop a professional development plan

US and Canada 301.654.SANS (7267) | EMEA and APAC inquiries: + 44 (0) 20 3598 2363

What's Your Next Career Move?

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

STI offers two unique master's degree programs:

Master of Science in Information Security Engineering

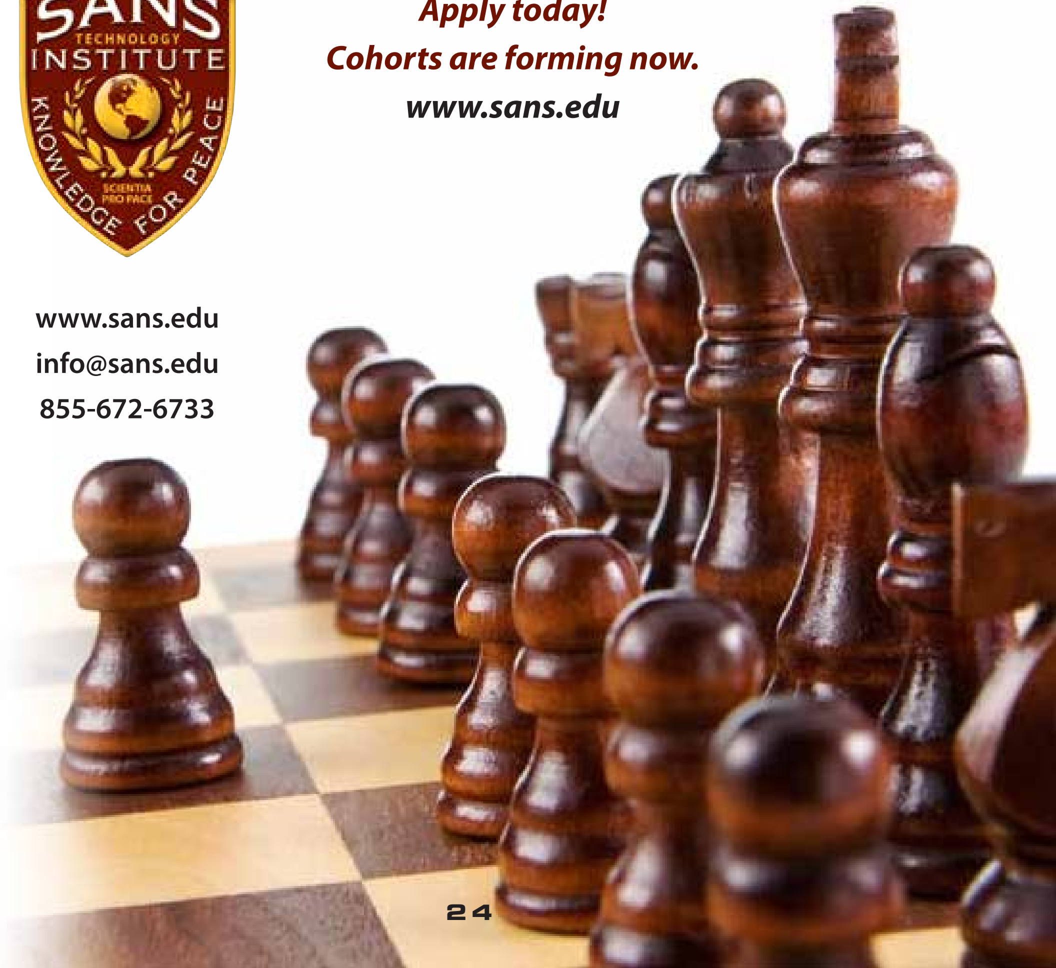
Master of Science in Information Security Management

"The STI master's degree program combines the best of administrative and technical security into the curriculum. When you achieve your degree, you're well versed and can address any and all challenges placed before you."

-Kevin Fuller, MSISE Student

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

Apply today!
Cohorts are forming now.
www.sans.edu



www.sans.edu
info@sans.edu
855-672-6733

ICS TRAINING AVAILABLE!

Industrial Control Systems

Asia Pacific ICS Security Summit

Singapore | SUMMIT: 2-3 December 2013 | POST_SUMMIT COURSES: 4-7 December 2013

The Summit brings together the program managers, control systems engineers, IT security professionals and critical infrastructure protection specialists from asset owning and operating organizations along with control systems and security vendors who have innovative solutions for improving security. It is the place to come and interact with top SCADA experts, key government personnel, researchers and asset owners at the multiple special networking events.

More than 1,500 security analysts and process control engineers, from government and industry, have attended the SCADA Security Summits. That's because the Summits are the one place where the people shaping the future of control systems security come together to share the lessons they have learned and because the Summits give attendees unique, early access to important new information. This year's program will be no different. If you have any responsibility for security of control systems – policy, engineering, governance or operations you won't want to miss the 2013 Summit in Singapore.

What You Will Learn

- Learn the most critical security challenges in implementing smart meters and smart grid. Learn what the US is doing with its $4.8 billion in Smart Grid funding to ensure these systems do not create new risks.
- Learn the lessons discovered by leading process control user organizations throughout the world, and what your process control vendor may be doing to boost the defenses on systems already deployed, and on new systems.
- Learn why control systems are so difficult to protect and arm yourself with clear case studies showing what has been done and what can be done to protect SCADA and other control systems. Learn the language of control systems so you can be of more help to the engineers who plan and deploy such systems.
- Understand the requirements and constraints faced by owners and operators of automation systems. Determine the state of the art in control system security as a benchmark for your own future planning.
- Better understand what government can and cannot do by learning the requirements, constraints, and current capabilities available to secure critical control systems.

Who Should Attend

- Plant Managers, Engineering and Operations Management, Project Managers, Automation and Control Managers, Process Control and SCADA Engineers, Plant Engineers
- Control System Vendor Developers and Integrators
- Information Security and IT Professionals in Organizations that Deploy Industrial Control Systems
- Government Leaders Responsible for Policy and Regulation of Utilities and Other Process Control Users
- Academic and Research Laboratory Leaders

> ***"Excellent learning experience – the panelists stayed on topic throughout and I got a good sense of the threat environment."***
>
> -Tom Pacha, Public Safety Canada

www.sans.org/event/asia-pacific-ics-security-summit-training

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

www.sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-learning available anytime, anywhere, at your own pace

www.sans.org/ondemand

vLive

Convenient online instruction from SANS' top instructors

www.sans.org/vlive

Simulcast

Attend a SANS training event without leaving home

www.sans.org/simulcast

CyberCon

Live online training event

www.sans.org/cybercon

SelfStudy

Self-paced online training for the motivated and disciplined infosec student

www.sans.org/selfstudy