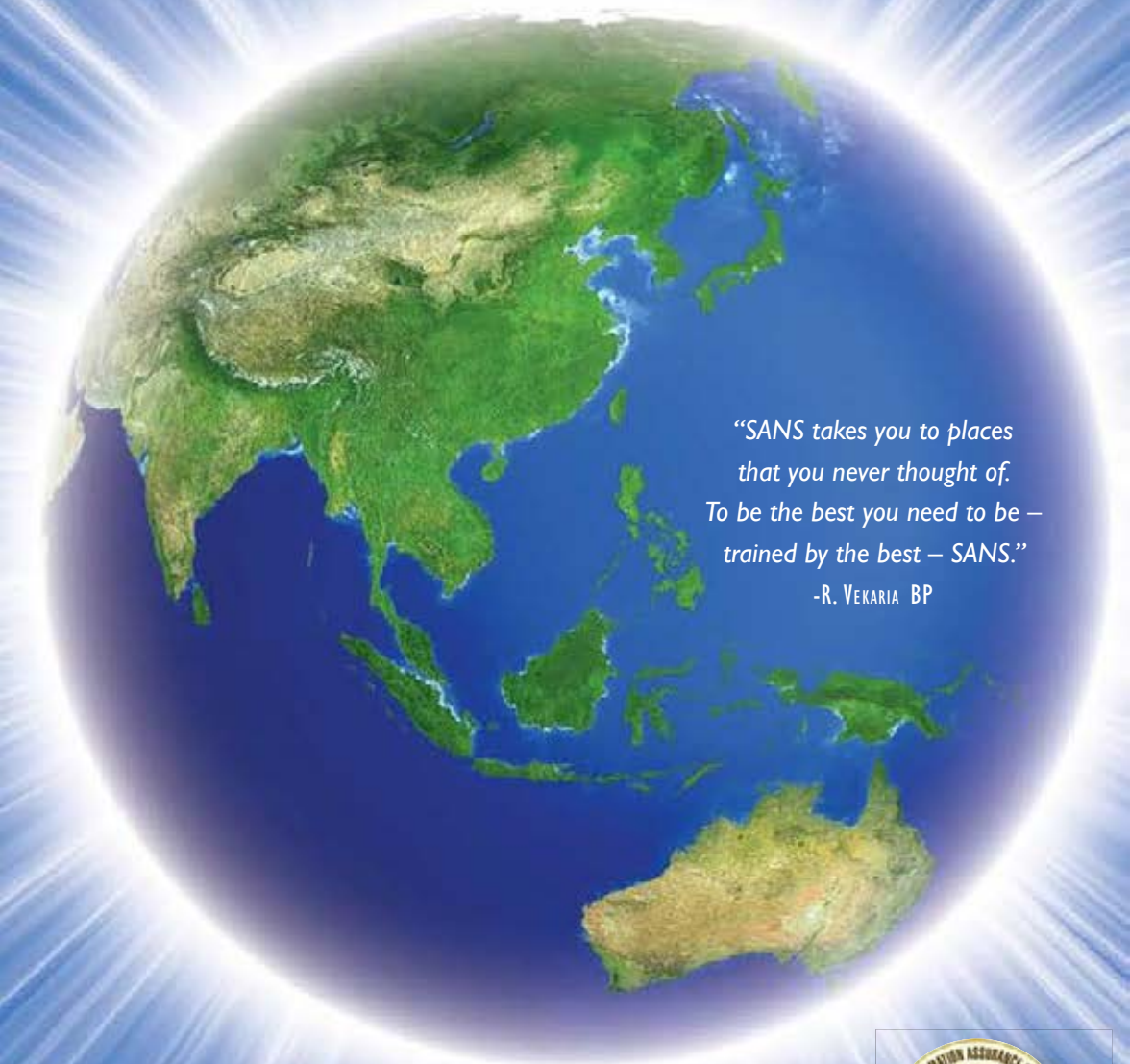
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS

2015 ASIA-PACIFIC
Course Catalog

Australia Hong Kong India Japan Korea Malaysia Singapore Thailand



"SANS takes you to places that you never thought of. To be the best you need to be – trained by the best – SANS."
-R. VEKARIA BP

REGISTER AT
sans.org

CONTACT US AT
AsiaPacific@sans.org
+65 69 339 540

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

ENTERPRISE
- **SEC560** Network Pen Testing and Ethical Hacking **GPEN**
- **SEC561** Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
- **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**
- **SEC760** Advanced Exploit Development for Penetration Testers

WEB
- **SEC542** Web App Pen Testing and Ethical Hacking **GWAPT**
- **SEC642** Advanced Web App Pen Testing and Ethical Hacking

WIRELESS
- **SEC575** Mobile Device Security and Ethical Hacking **GMOB**
- **SEC617** Wireless Ethical Hacking, Pen Testing, and Defenses **GAWN**

SPECIALIZATION
- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise
- **SEC573** Python for Penetration Testers
- **SEC580** Metasploit Kung Fu for Enterprise Pen Testing

Network Operations Center, System Admin, Security Architecture

SEC401 Security Essentials Bootcamp Style **GSEC**

- **SEC501** Advanced Security Essentials – Enterprise Defender **GCED**
- **SEC505** Securing Windows with the Critical Security Controls **GCWN**
- **SEC506** Securing Linux/Unix **GCUX**
- **SEC566** Implementing and Auditing the Critical Security Controls **GCCC**
- **SEC579** Virtualization and Private Cloud Security

Security Operations Center/Intrusion Detection

SEC401 Security Essentials Bootcamp Style **GSEC**

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

ENDPOINT MONITORING
- **SEC501** Advanced Security Essentials – Enterprise Defender **GCED**
- **FOR508** Advanced Computer Forensic Analysis & Incident Response **GCFA**

SPECIALIZATION
- **SEC502** Perimeter Protection In-Depth **GPPA**
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **SEC511** Continuous Monitoring and Security Operations

AUDIT CURRICULUM

- **AUD480** Top 4 Mitigation Strategies: Implementing and Auditing
- **SEC566** Implementing and Auditing the Critical Security Controls – In-Depth **GCCC**
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

FORENSICS CURRICULUM

Incident Response

SEC401 Security Essentials Bootcamp Style **GSEC**

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

NETWORK ANALYSIS
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **FOR572** Advanced Network Forensics and Analysis **GNFA**

ENDPOINT ANALYSIS
- **FOR408** Windows Forensic Analysis **GCFE**
- **FOR508** Advanced Computer Forensic Analysis and Incident Response **GCFA**

MALWARE ANALYSIS
- **FOR610** Reverse Engineering Malware: Malware Analysis Tools and Techniques **GREM**

SPECIALIZATION
- **FOR526** Memory Forensics In-Depth
- **FOR559** Cloud Forensics and Incident Response
- **MGT535** Incident Response Team Management

Digital Forensic Investigations

FOR408 Windows Forensic Analysis **GCFE**

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

- **FOR508** Advanced Computer Forensic Analysis and Incident Response **GCFA**
- **FOR585** Advanced Smartphone Forensics
- **FOR518** Mac Forensic Analysis
- **FOR526** Memory Forensics In-Depth
- **FOR610** Reverse Engineering Malware: Malware Analysis Tools and Techniques **GREM**

LEGAL CURRICULUM

- **SEC401** Security Essentials Bootcamp Style **GSEC**
- **LEG523** Law of Data Security and Investigations **GLEG**

ICS CURRICULUM

- **ICS410** ICS/SCADA Security Essentials **GICSP**

MANAGEMENT CURRICULUM

- **SEC301** Intro to Information Security **GISF**
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ **GSLC**
- **MGT535** Incident Response Team Management
- **MGT433** Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

- **SEC401** Security Essentials Bootcamp Style **GSEC**
- **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep **GCPM**
- **MGT414** SANS® +S™ Training Program for the CISSP® Certification Exam **GISP**
- **MGT514** IT Security Strategic Planning, Policy, and Leadership

DEVELOPER CURRICULUM

CORE
- **Securing the Human for Developers** Application Security Awareness Modules
- **DEV522** Defending Web Applications Security Essentials **GWEB**

SECURE CODING
- **DEV541** Secure Coding in Java/JEE **GSSP-JAVA**
- **DEV544** Secure Coding in .NET **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
- **SEC575** Mobile Device Security and Ethical Hacking **GMOB**

For information on all of SANS' courses, visit sans.org/courses

GIAC certification available for courses indicated with GIAC acronyms

SANS Asia-Pacific 2015 Event Schedule

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

AUSTRALIA

	SEC401 Security Essentials Bootcamp Style	SEC480 Top 4 Mitigation Strategies: Implementing & Auditing	SEC501 Advanced Security Essentials – Enterprise Defender	SEC502 Perimeter Protection In-Depth	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	SEC542 Web App Penetration Testing and Ethical Hacking	SEC560 Network Penetration Testing and Ethical Hacking	SEC561 Intense Hands-on Pen Testing Skill Development (with SANS NetWars)	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	FOR408 Windows Forensic Analysis	FOR508 Advanced Computer Forensic Analysis and Incident Response	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	ICS410 ICS/SCADA Security Essentials
Secure Canberra Canberra • 23-28 Mar	SEC401 *Page 6*				SEC504 *Page 11*		SEC542 *Page 13*					FOR408 *Page 21*			
Melbourne Melbourne • 18-23 May	SEC401 *Page 6*				SEC504 *Page 11*								FOR508 *Page 22*		
Canberra Canberra • 30 Jun - 11 Jul	SEC401 *Page 6*	SEC480 *Page 7*		SEC502 *Page 9*		SEC511 *Page 12*		SEC560 *Page 14*		SEC575 *Page 16*				FOR610 *Page 26*	
Sydney Sydney • 9-21 Nov	SEC401 *Page 6*		SEC501 *Page 8*		SEC504 *Page 11*				SEC561 *Page 15*		SEC660 *Page 19*				ICS410 *Page 28*

SINGAPORE

	SEC401 Security Essentials Bootcamp Style	SEC502 Perimeter Protection In-Depth	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	SEC542 Web App Penetration Testing and Ethical Hacking	SEC560 Network Penetration Testing and Ethical Hacking	SEC561 Intense Hands-on Pen Testing Skill Development (with SANS NetWars)	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	SEC760 Advanced Exploit Development for Penetration Testers	FOR508 Advanced Computer Forensic Analysis and Incident Response	FOR518 Mac Forensic Analysis	FOR572 Advanced Network Forensics and Analysis	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Secure Singapore Singapore • 9-21 Mar			SEC504 *Page 11*	SEC511 *Page 12*	SEC542 *Page 13*		SEC561 *Page 15*			SEC760 *Page 20*			FOR572 *Page 25*	FOR610 *Page 26*
October Singapore Singapore • 19-24 Oct	SEC401 *Page 6*	SEC502 *Page 9*				SEC560 *Page 14*		SEC575 *Page 16*	SEC660 *Page 19*		FOR508 *Page 22*	FOR518 *Page 23*		

JAPAN

	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC561 Intense Hands-on Pen Testing Skill Development	FOR508 Advanced Computer Forensic Analysis and Incident Response
Tokyo Tokyo • 9-14 Nov	SEC504 *Page 11*	SEC561 *Page 15*	FOR508 *Page 22*

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

SANS Asia-Pacific 2015 Event Schedule

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

INDIA	SEC401 Security Essentials Bootcamp Style	SEC503 Intrusion Detection In-Depth	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	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	SEC642 Advanced Web App Penetration Testing and Ethical Hacking	SEC660 Adv. Pen Testing, Exploit Writing, and Ethical Hacking	FOR408 Windows Forensic Analysis	FOR526 Memory Forensics In-Depth	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	ICS410 ICS/SCADA Security Essentials
Secure India Bangalore • 23 Feb - 7 Mar	SEC401 *Page 7*	SEC503 *Page 10*	SEC504 *Page 11*											
Delhi Delhi • 24 Aug - 5 Sep											FOR408 *Page 21*	FOR526 *Page 24*	FOR610 *Page 26*	
Bangalore Bangalore • 29 Sep - 11 Oct				SEC511 *Page 12*		SEC560 *Page 14*	SEC575 *Page 16*	SEC579 *Page 17*	SEC642 *Page 18*					
Hyderabad Hyderabad • 23-28 Nov					SEC542 *Page 13*					SEC660 *Page 19*				ICS410 *Page 28*

SOUTHEAST ASIA	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC560 Network Penetration Testing and Ethical Hacking	FOR408 Windows Forensic Analysis
Secure Thailand Bangkok • 25-30 May		SEC560 *Page 14*	FOR408 *Page 21*
Malaysia Kuala Lumpur • 24-28 Aug	SEC504 *Page 11*		

KOREA	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC560 Network Penetration Testing and Ethical Hacking	FOR508 Advanced Computer Forensic Analysis and Incident Response	AUD507 Auditing & Monitoring Networks, Perimeters, and Systems
Cyber Defense Korea Seoul • 27 Apr - 2 May		SEC560 *Page 14*		AUD507 *Page 27*
Korea Seoul • 14-19 Sep	SEC504 *Page 11*		FOR508 *Page 22*	

HONG KONG	SEC542 Web App Penetration Testing and Ethical Hacking	FOR508 Advanced Computer Forensic Analysis and Incident Response
Hong Kong Hong Kong • 7-12 Sep	SEC542 *Page 13*	FOR508 *Page 22*

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
46 CPEs
Laptop Required
- GIAC Cert: GSEC
- Masters Program

TRAINING EVENTS:
- Secure India
- Secure Canberra
- Melbourne
- Canberra
- October Singapore
- Sydney

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 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. The course 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 addition 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 cybersecurity. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

"SEC401 is the best InfoSec training bar none. The value for the money is unbeatable!"
-Ron Foupht, Sirius Computer Solutions

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 cybersecurity. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

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

"SEC401 is an eye opener to the broader aspects of network/ security admin roles. You see things from a different paradigm."
-Rod Campbell, CITEC

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.

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

You Will Be Able To

- Design and build a network architecture using VLAN's, NAC and 802.1x based on an 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 prepare a checklist to validate 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

giac.org

sans.edu

SECURITY 480

Top 4 Mitigation Strategies: Implementing and Auditing

NEW

SANS

Three-Day Program
18 CPEs
Laptop Required

TRAINING EVENTS:
- Canberra

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

There has been a significant push for public and private sector organisations to implement the Top 4 Mitigation Strategies which are:

1. **Application Whitelisting;**
2. **Patch Applications;**
3. **Patch Operating System;**
4. **Minimise Administrative Privileges.**

The Cyber Security Operations Centre in ASD has stated that at least 85% of the cyber intrusions it responds to would be mitigated had agencies implemented these Top 4 strategies. For security professionals, this course enables you to practically implement these strategies in in your existing network using a variety of technologies and methods. For auditors, CIOs and risk officers this course is the best way to understand how to measure if the Top 4 mitigation strategies have been effectively implemented in an organisation.

After attending this hands-on course, individuals will be able to effectively implement and audit the Top 4 mitigation strategies in their own environments to achieve a significant level of security. This course closely aligns with the ASD Top 4 mitigation strategies which can be found here: www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

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

- Understand the techniques attackers use in targeted cyber intrusions
- Learn the importance of the Top 4 mitigation strategies including their effectiveness
- Gain a sound understanding of the strategies, their objectives and compliance requirements
- Obtain practical experience installing, configuring and deploying technologies to implement the Top 4 Mitigation Strategies
- Understand common implementation roadblocks and methods to overcome them
- Learn implementation and business communication methods
- Learn how to protect your systems from targeted cyber intrusions
- Learn how to detect targeted cyber intrusions
- Learn how to implement business processes which support the Top 4 mitigation strategies

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GCED
- Masters Program

TRAINING EVENTS:
- Sydney

Cybersecurity continues to be a critical area for organizations and will increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

"Great course. Best training I have attended. This is my first SANS course and I can't wait to attend more."
-Leonard Crull, MI ANG

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks will continue to pose a threat to an organization as data become more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

"Very knowledgeable. Top-tier training and industry leading."
-Herbert Monford, Regions Bank

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

"It identifies and demonstrates a wide variety of attack factors that can be leveraged to steal my company's data."
-Corey Bidne, USDA

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want broad, advanced coverage of the core areas to protect their systems
- Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Learn the tools that can be used to analyze a network to both prevent and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Understand the six steps in the incident handling process and be able to create and run an incident handling capability
- Learn how to use various tools to identify and remediate malware across your organization
- Create a data classification program and be able to deploy data loss prevention solutions at both a host and network level

giac.org

sans.edu

SECURITY 502

Perimeter Protection In-Depth

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GPPA
- Masters Program

TRAINING EVENTS:
- Canberra
- October Singapore

There is no single fix for securing your network. That's why this course is a comprehensive analysis of a wide breadth of technologies. In fact, this is probably the most diverse course in the SANS catalog, as mastery of multiple security techniques is required to defend your network from remote attacks. You cannot just focus on a single OS or security appliance. A proper security posture must be comprised of multiple layers. This course was developed to give you the knowledge and tools necessary at every layer to ensure your network is secure.

"As an analyst, these courses are the most relevant in the industry."
-Louis Robichaud, Atlantic Lottery Corp.

The course material has been developed using the following guiding principles:

- **Learn the process, not one specific product**
- **You learn more by doing, so hands-on problem-solving is key**
- **Always peel back the layers and identify the root cause**

The course starts by looking at common problems we need to resolve. Is there traffic passing by my firewall I didn't expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We'll dig into these questions and more and answer them.

We spend quite a bit of time learning about IP. Sure we all know how to assign an IP address, but to secure your network you really need to understand the idiosyncrasies of the protocol. We'll talk about how IP works and how to spot the abnormal patterns. If you can't hear yourself saying "Hummm, there are no TCP options in that packet. It's probably forged," then you'll gain some real insight from this portion of the material.

Once you have an understanding of the complexities of IP, we'll get into how to control it on the wire. Rather than trying to tell you what are good and bad products, we focus on the underlying technology used by all of them. This is extremely practical information because a side-by-side product comparison is only useful for that specific moment in time. By gaining knowledge of what goes on under the cover, you will be empowered to make good product choices for years to come. Just because two firewalls are stateful inspection, do they really work the same on the wire? Is there really any difference between stateful inspection and network-based intrusion prevention, or is it just marketing? These are the types of questions we address in this portion of the course.

From there, it's a hands-on tour through how to perform a proper wire-level assessment of a potential product, as well as what options and features are available. We'll even get into how to deploy traffic control while avoiding some of the most common mistakes. Feel like your firewall is generating too many daily entries for you to review the logs effectively? We'll address this problem not by reducing the amount of critical data, but by streamlining and automating the backend process of evaluating it.

But you can't do it all on the wire. A properly layered defense needs to include each individual host – not just the hosts exposed to access from the Internet, but hosts that have any kind of direct or indirect Internet communication capability as well. We'll start with OS lockdown techniques and move on to third-party tools that can permit you to do anything from sandbox insecure applications to full-blown application policy enforcement.

While technical knowledge is important, what really matters are the skills to properly leverage it. This is why the course is heavily focused on problem solving and root cause analysis. While these are usually considered soft skills, they are vital to being effective in the role of security architect.

Who Should Attend

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network and system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

"SEC502 opened my eyes so wide, it scared me!"
-George Scarborough, Defense Logistics Agency

You Will Be Able To

- Apply perimeter security solutions in order to identify and minimize weaknesses to properly protect your perimeter
- Deploy and utilize multiple firewalls to understand the strengths and weaknesses that each presents
- Use built-in tools to audit, protect and identify if systems have been compromised
- Utilize tcpdump to analyze network traffic in detail to understand what packets are communicating and how to identify potential covert channels
- Understand and utilize techniques to compromise and protect against application layer attacks such as XSS, CSRF, SQL injection and more
- Utilize tools to evaluate packets and identify legitimate and illegitimate traffic
- Use tools to evaluate and identify the risks related to Cloud Computing
- Inspect the intricate complexities of IP, including identifying malicious packets
- Evaluate and secure SSL, wireless networks, VPNs, applications and more
- Implement a logging solution that properly identifies risk and is manageable

giac.org

sans.edu

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GCIA
- Masters Program

TRAINING EVENTS:
- Secure India

If you have an inkling of awareness of security (even my elderly aunt whose idea of a mobile device is a wheelchair, knows about the perils of the Interweb), you often hear the disconcerting news about another compromise at a high-profile company. 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 creating an environment to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth track – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

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

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.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. Packetrix is supplemented with demonstration "pcaps" – files that contain network traffic. This allows the student to follow along on her/his laptop with the class material and demonstrations. Additionally, these pcaps provide a good library of network traffic to use when reviewing the material, especially for certification.

"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

There are several hands-on exercises each day to reinforce the course book material, allowing you to transfer the knowledge in your head to execution at your keyboard.

Exercises have two different approaches – a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for exercises intended to challenge the most advanced student.

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

The challenging hands-on exercises are specially designed to be valuable for all experience levels. The Packetrix VMware used in class is a Linux distribution so we strongly recommend that you spend some time getting familiar with a Linux environment that uses the command line for entry, along with learning some of the core Unix commands before coming to class.

Who Should Attend

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

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

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

GCIA
giac.org

SANS INSTITUTE
sans.edu

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
37 CPEs
Laptop Required
- GIAC Cert: GCIH
- Masters Program

TRAINING EVENTS:
- Secure India
- Secure Singapore
- Secure Canberra
- Melbourne
- Malaysia
- Korea
- Tokyo
- Sydney

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.

"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

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.

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

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.

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 choose appropriate response actions based on each attacker's flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

"SEC504 opens your eyes to the real cyberworld. It encourages thinking about security of data and network access."
-Frank Munson, Virginia International Terminal

giac.org

sans.edu

SECURITY 511

Continuous Monitoring and Security Operations

NEW

SANS

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS:
- Secure Singapore
- Canberra
- Bangalore

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

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

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring (CSM), taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and Day five (5) will greatly increase your understanding and enhance your skills in implementing Continuous Monitoring utilizing NIST framework.

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification (GSE). Both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the capture-the-flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Who Should Attend

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

You Will Be Able To

- Learn the critical components of a Security Operations Center (SOC)
- Understand the principles of a defensible security architecture
- Draw on hands-on experience applying current security countermeasures
- Apply a framework for security analysis and monitoring to a SOC
- Analyze a security architecture for deficiencies
- Build security visibility into virtualized environments
- Define security requirements for a SOC with Continuous Monitoring
- Determine appropriate security monitoring needs for organizations of all sizes
- Determine requisite monitoring capabilities for SOC environments
- Detect and understand modern post-exploitation activity
- Understand current attack techniques and how they circumvent traditional architectures
- Correlate security monitoring data for actionable intelligence
- Design a defensible security architecture
- Design a SOC that provides enterprise visibility
- Understand the need and benefits of Continuous Security Monitoring and Continuous Diagnostics and Mitigation
- Write scripts to reduce the TCO of continuous security monitoring
- Implement a robust Continuous Security Monitoring program
- Instrument Continuous Security Monitoring in a SOC environment
- Perform key aspects of Continuous Diagnostics and Mitigation

SECURITY 542

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GWAPT
- Masters Program

TRAINING EVENTS:
- Secure Singapore
- Secure Canberra
- Hong Kong
- Hyderabad

Assess Your Web Apps in Depth

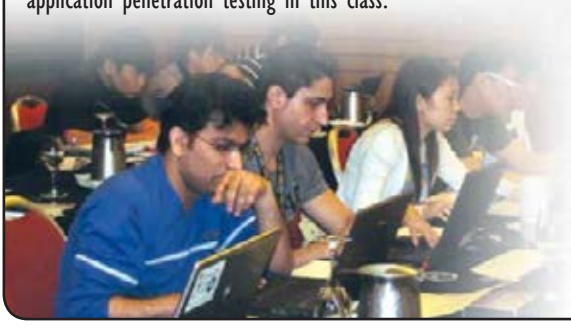
"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, i2P LLC

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.

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.



"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

Who Should Attend

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

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 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

GWAPT
giac.org

SANS INSTITUTE
sans.edu

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
37 CPEs
Laptop Required
- GIAC Cert: GPEN
- Masters Program

TRAINING EVENTS:
- Cyber Defense Korea
- Secure Thailand
- Canberra
- October Singapore
- Bangalore

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

"SEC560 presents great content, real world expertise and application."
-Brice Toth, PSU

THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

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

"Learning all these tools is super valuable for security professionals or even system admins, they help understand how things work."
-Igor Guarisma

You will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. You'll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post exploitation, password attacks, wireless, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

With comprehensive coverage of tools, techniques, and methodologies for network, web app, and wireless testing, SEC560 truly prepares you to conduct high-value penetration testing projects end-to-end, step-by-step. Every organization needs skilled infosec personnel who can find vulnerabilities and mitigate their impacts, and this whole course is specially designed to get you ready for that role. With over 30 detailed hands-on labs through- out, the course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job masterfully, safely, and efficiently.

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

giac.org

sans.edu

SECURITY 561

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

SANS

Six-Day Program
36 CPEs
Laptop Required

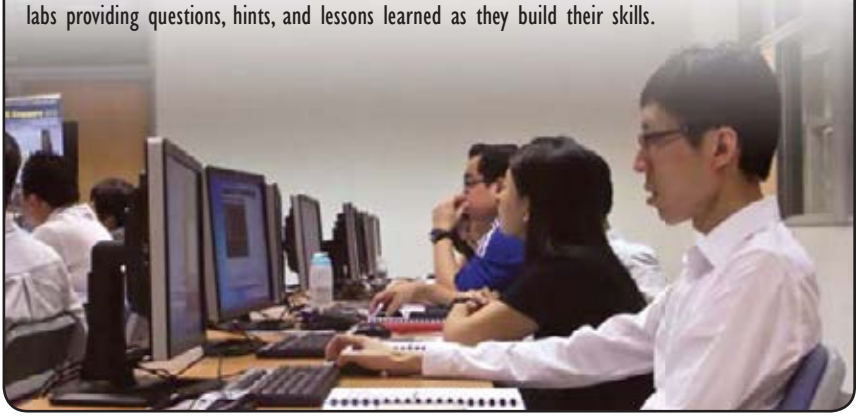
TRAINING EVENTS:
- Secure Singapore
- Tokyo
- Sydney

To be a top pen test professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. SANS' top instructors engineered SEC561: Intense Hands-on Pen Testing Skill Development from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises and labs, maximizing keyboard time on in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical hands-on skills needed to address today's pen test and vulnerability assessment projects in enterprise environments.

To get the most out of this course, students should have at least some prior hands-on vulnerability assessment or penetration testing experience (at least 6 months) or have taken at least one other penetration testing course (such as SANS SEC504, SEC560, or SEC542). The course will build on that background, helping participants ramp up their skills even further across a broad range of penetration testing disciplines.

Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios that they can apply the day they get back to their jobs.

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



Who Should Attend

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defense techniques
- Forensic analysts who need to improve their 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
- Manipulate 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

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GMOB
- Masters Program

TRAINING EVENTS:
- Canberra
- Bangalore
- October Singapore

Now covering BlackBerry 10, Apple iOS 7, and Android 4.3 devices

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.

"The content of SEC575 is simply eye-opening. Organizations are so busy trying to roll out their BYOD projects without any understanding of the risks. This course is a must for security professionals rolling out BYOD projects."
-Vijay Kora, Open Solutions Consulting Inc.

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

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

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and from 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 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

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

"This is eye-opening material! I am mesmerized by this course. It's time to test apps, because they can't be trusted."
-Matthew Britton, BCBSLA

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, 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, dextranslator, 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

giac.org

sans.edu

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS:
- Bangalore

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

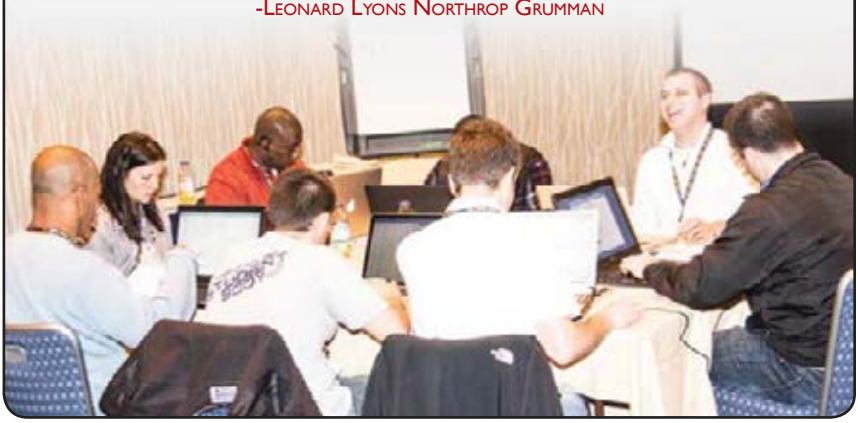
With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand,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

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

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

"SEC579 is the absolute best virtualization security information available! And it's immediately usable."
-Leonard Lyons Northrop Grumman



"SEC579 actually provides pertinent information outside what is freely available and is applicable to securing my organization's virtual infrastructure."
-David Richardson, ManTech

"The rush for virtualization is difficult for security sensitive environments. SEC579 helps demonstrate which risks are valid."
-Paul Mayers, Lloyds Banking Group

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 ac- quire forensic evidence
- Perform audits and risk assessments within a virtual or private cloud environment

SECURITY 642

Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS:
- Bangalore

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag event, which tests the knowledge you will have acquired during the previous five days.

"Outstanding course!! It is great to have an opportunity to learn the material from someone who is extremely relevant in the field and is able to impart the value of his experiences."
-Bobby Bryant, DoD

We will begin by exploring advanced techniques and attacks to which modern, complex applications are vulnerable. We will then explore encryption as it relates to web applications, digging deep into practical cryptography including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing this encryption. We will spend some time looking at alternate front ends to web applications and web services such as mobile applications. The final portion of the class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system.

The SANS promise is that you will be able to use these ideas immediately upon returning to the office in order to better perform penetration tests of your web applications and related infrastructure. This course will enhance your exploitation and defense skill sets and fulfills a need to teach more advanced techniques than can be covered in the foundational course, *SEC542: Web Application Penetration Testing and Ethical Hacking.*

Who Should Attend

- Web penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

"SEC642 is a great way to take your testing to the next level. I can't wait to try everything when I get back to work."
-Sara Dunnack, Aetna

"SEC642 is very relevant to the work I do everyday, and provides a lot of insight into technologies I thought I was familiar with."
-John Lincoln, Nordstrom

You Will Be Able To

- Assess and attack complex modern applications
- Understand the special testing and exploits available against content management systems such as SharePoint and WordPress
- Use techniques to identify and attack encryption within applications
- Identify and bypass web application firewalls and application filtering techniques to exploit the system
- Use exploitation techniques learned in class to perform advanced attacks against web application flaws such as XSS, SQL injection and CSRF

SECURITY 660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GXPN
- Masters Program

TRAINING EVENTS:
- October Singapore
- Sydney
- Hyderabad

This course is designed as a logical progression point for those who have completed *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!

"Looking at everything I have learned from SANS, I definitely feel I have gained an edge when it comes to the augmentation of my pentest skills."
-Alexander Cobblah, Booz Allen Hamilton

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

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. 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 the advanced penetration concept, and provides 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.

"The CTF with teams was awesome!!! I learned a lot more when working through some of the issues with my peers."
-Mike Evans, Alaska Airlines

"SEC660 is actually a technical class and not 'fad' info security garbage everyone else is teaching."
-Kyle Hanslovan, ManTech

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

giac.org

sans.edu

SECURITY 760

Advanced Exploit Development for Penetration Testers

NEW

SANS

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS:
- Secure Singapore

Who Should Attend

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

What You Will Receive

- You will receive various preconfigured *NIX virtual machines; however, you are required to bring the aforementioned Windows VMs
- You will receive various tools on a course DVD that are required for use in class

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. 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 one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7 and 8 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

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
- Jump into Windows kernel exploitation

"SEC760 is the kind of training we couldn't get anywhere else. It's not all theory, we got to implement and to exploit everything we learned."

-Jenny Kitaichit, Intel

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GCFE
- Masters Program

TRAINING EVENTS:
- Secure Canberra
- Secure Thailand
- Delhi

Master computer forensics. What Do You Want to Uncover Today?

"Hands down the BEST forensics class EVER!! Blew my mind at least once a day for 6 days!"
-Jason Jones, USAF

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

FOR408: Windows Forensic Analysis focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know 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 could be used internally or in civil/criminal litigation.

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

This course utilizes a brand-new Windows 8.1 based case exercise that took over 6 months to create the data. Realistic example case data takes months to create in real time correctly. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. Our development team spent months creating an incredibly realistic scenario. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The brand new case workbook, will detail the step-by-step each investigator could follow to examine the latest technologies including Windows 8.1.

"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

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 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, including how and who placed an artifact on the system, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry analysis, Windows artifact analysis, and email analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), email analysis, and Windows Registry parsing
- Use automated analysis techniques via AccessData's Forensic ToolKit (FTK)
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information that the suspect was interested in finding and to accomplish damage assessments
- Use shellbags analysis tools to articulate every folder and directory that a user opened up while browsing the hard drive
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- Learn event log analysis techniques and use them to determine when and how users logged into a Windows system via a remote session, at the keyboard, or simply by unlocking their screensaver
- Determine where a crime was committed using FTK Registry Viewer to pinpoint the geo-location of a system by examining connected networks, browser search terms, and cookie data
- Use Mandiant Web Historian, parse raw SQLite databases, and leverage browser session recovery artifacts and flash cookies to identify web activity of suspects, even if privacy cleaners and in-private browsing are used

digital-forensics.sans.org

giac.org

sans.edu

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GCFA
- Masters Program

TRAINING EVENTS:
- Melbourne
- Hong Kong
- Korea
- October Singapore
- Tokyo

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

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

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

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

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

"Everything you need to learn for the basics of forensics in just six days; any more knowledge and your head would explode!"
-Matthew Harvey, U.S. Department of Justice

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

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

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, and 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 it has 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, and 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

DFIR
digital-forensics.sans.org

GCFA
giac.org

SANS INSTITUTE
sans.edu

FORENSICS 518

Mac Forensic Analysis

NEW

SANS

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS:
- October Singapore

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

FORENSICATE DIFFERENTLY!

The FOR518: Mac Forensic Analysis Course will teach you:

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

"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."
-Naveel Koya, A C-DAC - Trivandrum

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

"Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."
-Kevin J. Ripa, Computer Evidence Recovery, Inc.

DFIR

digital-forensics.sans.org

Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, or detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR408, FOR508, FOR526, FOR610, FOR585 alumni looking to round out their forensic skills

FORENSICS 526

Memory Forensics In-Depth

NEW

SANS

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS:
- Delhi

Digital Forensics and Incident Response (DFIR) professionals view the acquisition and analysis of physical memory as critical to the success of an investigation, be it a criminal case, employee policy violation, or enterprise intrusion. Investigators who do not look at volatile memory are leaving evidence on the table. The valuable contents of RAM hold evidence of user actions as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526 provides the critical skills necessary for digital forensics examiners and incident responders to deftly analyze captured memory images and live response audits. By using the most effective freeware and open-source tools in the industry today and delivering a deeper understanding of how these tools work, this five-day course shows DFIR professionals how to unravel the real story of what happened on a system. It is a critical course for any serious investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

Just as it is crucial to understand disk and registry structures to substantiate findings in traditional system forensics, it is equally critical to understand memory structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand.

Remember: "Malware can hide, but it must run." It is this malware paradox that is the key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible for them to hide their footprints completely from a skilled incident responder performing memory analysis. FOR526 will ensure that you and your team are ready to respond to the challenges inherent in DFIR by using cutting-edge memory forensics tools and techniques.

"The training opened my eyes for the need to collect memory images as well as physical images for single computer analysis such as theft of IP or other employee investigations."
-Greg Caouette, Kroll

FOR526 Memory Forensics In-Depth will teach you:

- **Proper Memory Acquisition:** Demonstrate targeted memory capture ensuring data integrity and combating anti-acquisition techniques.
- **How to Find Evil in Memory:** Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms.
- **Effective Step-by-Step Memory Analysis Techniques:** Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior.
- **Best Practice Techniques:** Learn when to implement triage, live system analysis, and alternative acquisition techniques, and how to devise custom parsing scripts for targeted memory analysis.

DFIR

digital-forensics.sans.org

Who Should Attend

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- 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 with a net- work 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 SysInternals 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 search- ing, 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

FORENSICS 572

Advanced Network Forensics & Analysis

NEW

SANS

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS:
- Secure Singapore

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS Security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from 408 and 508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

"FOR572 taught me how to use different evidence sources to fill in missing gaps. This is critical, as most environments or incidents will not have every type of evidence available."
-Alexander Bond, Mandiant

digital-forensics.sans.org

Who Should Attend

- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- IT lawyers and paralegals
- Anyone interested in computer network intrusions and investigations

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify an attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Use visualization tools and techniques to distill vast, complex data sources into management-friendly reports
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone exercise, modeled after real-world nation-state intrusions

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GREM
- Masters Program

TRAINING EVENTS:
- Secure Singapore
- Delhi
- Canberra

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 know 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!

"The exercises and examples are very good and useful to get a better understanding of code analysis. Definitely one of the best courses I've attended on this topic."
-Thor Olsen, Norwegian Police Security Services

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 and 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.

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.

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

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 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.

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

DFIR
digital-forensics.sans.org

GREM
giac.org

SANS INSTITUTE
sans.edu

AUDIT 507

Auditing & Monitoring Networks, Perimeters, and Systems

SANS

Six-Day Program
36 CPEs
Laptop Required
- GIAC Cert: GSNA
- Masters Program

TRAINING EVENTS:
- Cyber Defense Korea

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.

"By far, this is the most hands-on, technical tool-oriented auditing class I have ever seen. I cannot imagine another class that forces you to use real tools in real situations. It is just like gaining real world experience."
-Jay Russell, U.S. Navy

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.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these 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.

"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

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

giac.org

sans.edu

INDUSTRIAL CONTROL SYSTEMS 410

ICS/SCADA Security Essentials

SANS

Five-Day Program
30 CPEs
Laptop Required
- GIAC Cert: GICSP

TRAINING EVENTS:
- Sydney
- Hyderabad

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

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints.
- Hands-on lab learning experiences to control system attack surfaces,methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals.

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

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

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

"Excellent content and very informative."
–Khalid Alsomaly, Saudi Aramco

giac.org

Who Should Attend

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

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with your Peers

Community SANS sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

OnSite sans.org/onsite
Live Training at Your Office Location

Mentor sans.org/mentor
Live Multi-Week Training with a Mentor

Summit sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive sans.org/vlive
Online, Evening Courses with SANS' Top Instructors

Simulcast sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SECURITY AWARENESS

SUMMIT & TRAINING 2015

Canberra

SUMMIT: **19 March**

TRAINING: **17-18 March**

Contact AsiaPacific@sans.org for details

SECURITY AWARENESS SUMMIT

The Security Awareness Summit & Training event combines hands-on classroom training with the Summit creating ONE premier event. Couple the two-day MGT433 course with the one-day action-packed Summit and take your Security Awareness skills to new levels. The ONLY Security Awareness training event on the SANS calendar! Join the most innovative minds in the industry to tackle advanced Security Awareness issues.

- Are you interested in taking your Security Awareness program to the next level?
- Have you wondered what other organizations are doing to effectively measure change in behavior and how they are making the most of their limited resources?
- Would you like to know the strategies and techniques organizations use to actively engage their employees and staff?

If you answered yes to any of these questions, the summit is the event for you. You will hear the answers to these questions and many more.

COURSE OFFERING

MANAGEMENT 433

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

Two-Day Course | Tue, 17 Mar – Wed, 18 Mar | 9:00am - 5:00pm | Laptop NOT Needed | Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little, if anything, into securing the human element. As a result, people are now the weakest link; the simplest way for cyber attackers to hack into any organization is to target your employees. One of the most effective ways to secure the human element is to build an active awareness and education program that goes beyond just compliance and changes behaviors. In this challenging course you will learn how to do just that. You will learn the key concepts and skills needed to build, maintain and measure a high-impact security awareness program. All course content is based on lessons learned from hundreds of organizations around the world. In addition, you will learn not only from extensive interaction with the instructor, but from working with your peers, as well. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so that you can immediately implement your own customized awareness program upon returning to your organization.