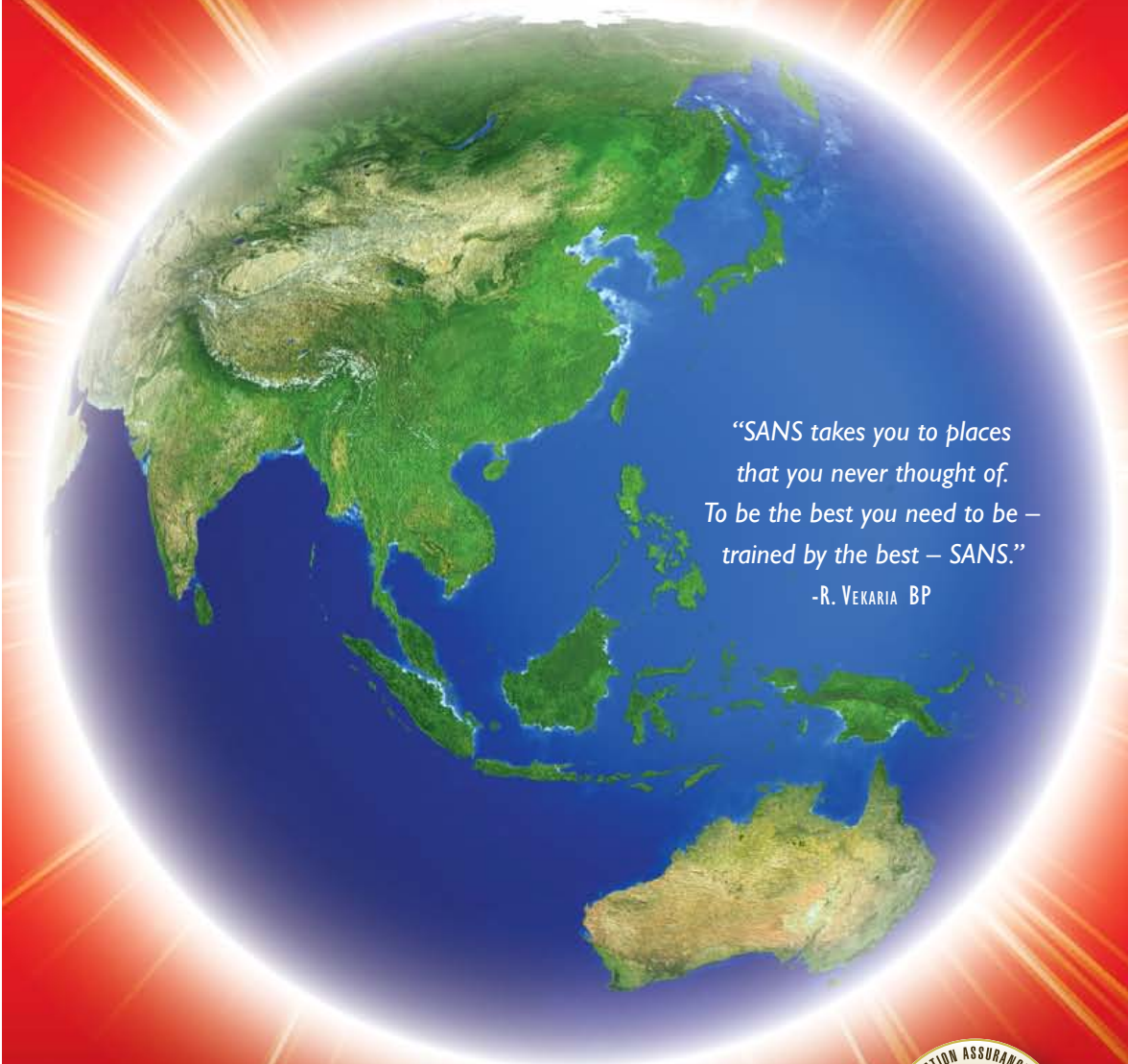
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS

2016 ASIA-PACIFIC
Course Catalog

AUSTRALIA INDIA JAPAN MALAYSIA PHILIPPINES SINGAPORE



"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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

GIAC Approved Training

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

Private
sans.org/private
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

Can't travel to a live SANS event?

Use SANS OnDemand to complete your training anytime, anywhere, at your own pace!

OnDemand

Learn more at
sans.org/ondemand

More than 30 SANS courses are available via OnDemand, all featuring:

- Four months of online course access
- Printed books and materials
- Labs, quizzes and archived lectures available 24/7
- Subject-matter expert support
- No Travel!

You can also bundle the features of OnDemand with live SANS event courses, giving you the best of both live and online SANS training.

PROVE YOUR SKILLS

STAY COMPETITIVE

GET GIAC CERTIFIED!

As an information security professional, it is critical to stay abreast of the latest techniques and demonstrate you have the skills to protect vital systems, data, and infrastructure.

GIAC is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by governments, militaries, and industries to protect their cyber environment..

Broad certifications don't cover hands-on technical skills like GIAC. There are over 30 certifications in cyber defense, forensics, penetration testing and ethical hacking, and management.

Dear Colleague,


Suresh Mustapha

We are pleased to share the SANS APAC 2016 course catalog to enable you and your colleagues to select the appropriate information security training classes at the most convenient time and location. For 2016, we have expanded our offering in Tokyo with **SANS Secure Japan 2016** in February, a pilot event in Manila – the inaugural **SANS Philippines 2016** in June, as well as a new event in the Australia roster – **SANS Adelaide 2016** in September. In addition to these new events and locations, we also have the following exciting new courses in our 2016 schedule:

ICS515: Industrial Control System Active Defense and Incident Response
This course will empower students with the ability to understand their networked industrial control system (ICS) environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. Students can expect to come out of this course fully understanding and able to deconstruct targeted ICS attacks, with a focus on delivery methods and observable attributes.

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

SEC561: Immersive Hands-On Hacking Techniques
To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. With over 30 hours of intense labs, SEC561 students experience a leap in their capabilities as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments.

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks.

SEC573: Python for Penetration Testers
This course will teach you the skills needed not only to tweak or customize tools, but to even develop your own tools from scratch. The course begins with an introduction to SANS pyWars, which is a four-day Capture-the-Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own pace. Experienced programmers can quickly progress to more advanced concepts while novice programmers spend time building a strong foundation.

FOR578: Cyber Threat Intelligence
During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578 will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

As always, please feel welcome to reach out to us at **AsiaPacific@sans.org** with any questions or suggestions!

Kindest regards,

Suresh Mustapha
MD Asia Pacific

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**

NETWORK & EXPLOITS	WEB	MOBILE/WIRELESS	LAB-CENTERED	SPECIALIZATION
SEC560 Network Pen Testing and Ethical Hacking **GPEN**	**SEC542** Web App Pen Testing and Ethical Hacking **GWAPT**	**SEC575** Mobile Device Security and Ethical Hacking **GMOB**	**SEC561** Immersive Hands-On Hacking Techniques	**SEC573** Python for Penetration Testers
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**	**SEC642** Advanced Web App Pen Testing and Ethical Hacking	**SEC617** Wireless Ethical Hacking, Pen Testing, and Defenses **GAWN**	**SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise	**SEC580** Metasploit Kung Fu for Enterprise Pen Testing
SEC760 Advanced Exploit Development for Penetration Testers				

Network Operations Center, System Admin, Security Architecture

SEC401 Security Essentials Bootcamp Style **GSEC**

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

SEC505 Securing Windows with PowerShell and 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 Digital Forensics and Incident Response **GCFA**

THREAT INTELLIGENCE

FOR578 Cyber Threat Intelligence

SPECIALIZATION

SEC502 Perimeter Protection In-Depth **GPPA**

SEC503 Intrusion Detection In-Depth **GCIA**

FOR572 Advanced Network Forensics and Analysis **GNFA**

SEC511 Continuous Monitoring and Security Operations **GMON**

SEC550 Active Defense, Offensive Countermeasures, and Cyber Deception

MANAGEMENT CURRICULUM

SEC301 Intro to Information Security **GISF**

SEC401 Security Essentials Bootcamp Style **GSEC**

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

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

MGT535 Incident Response Team Management

MGT414 SANS Training Program for CISSP® Certification **GISP**

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

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**

DEV541 Secure Coding in Java/JEE **GSSP-JAVA**

DEV544 Secure Coding in .NET **GSSP-.NET**

SPECIALIZATION

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

SEC642 Advanced Web App Pen Testing and Ethical Hacking

FORENSICS CURRICULUM

Incident Response

SEC401 Security Essentials Bootcamp Style **GSEC**

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

NETWORK ANALYSIS	ENDPOINT ANALYSIS	MALWARE ANALYSIS
SEC503 Intrusion Detection In-Depth **GCIA**	**FOR408** Windows Forensic Analysis **GCFE**	**FOR610** Reverse Engineering Malware: Malware Analysis Tools and Techniques **GREM**
FOR572 Advanced Network Forensics and Analysis **GNFA**	**FOR508** Advanced Digital Forensics and Incident Response **GCFA**	**FOR578** Cyber Threat Intelligence

SPECIALIZATION

FOR526 Memory Forensics In-Depth

MGT535 Incident Response Team Management

Digital Forensic Investigations

FOR408 Windows Forensic Analysis **GCFE**

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

FOR508 Advanced Digital Forensics 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**

AUDIT CURRICULUM

SEC480 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**

LEGAL CURRICULUM

SEC401 Security Essentials Bootcamp Style **GSEC**

LEG523 Law of Data Security and Investigations **GLEG**

ICS CURRICULUM

ICS410 ICS/SCADA Security Essentials **GICSP**

ICS515 ICS Active Defense and Incident Response

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

GIAC certification available for courses indicated with GIAC acronyms

SANS ASIA-PACIFIC 2016 EVENT SCHEDULE

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

AUSTRALIA

	SEC301 Intro to Information Security	SEC401 Security Essentials Bootcamp Style	SEC501 Advanced Security Essentials – Enterprise Defender	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 Hackinge	SEC550 Active Defense, Offensive Countermeasures and Cyber Deception	SEC560 Network Penetration Testing and Ethical Hacking	SEC561 Immersive Hands-On Hacking Techniques	SEC573 Python for Penetration Testers	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	FOR408 Windows Forensic Analysis	FOR508 Advanced Digital Forensics and Incident Response	FOR572 Advanced Network Forensics and Analysis	FOR578 Cyber Threat Intelligence	FOR610 REM: Malware Analysis Tools and Techniques	AUD507 Auditing & Monitoring Networks, Perimeters, and Systems	ICS410 ICS/SCADA Security Essentials	ICS515 ICS Active Defense and Incident Response	MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™
Secure Canberra Canberra • 18-23 Apr		SEC401 *Page 9*								SEC561 *Page 17*		SEC575 *Page 20*										MGT512 *Page 33*
Melbourne Melbourne • 16-21 May						SEC511 *Page 13*							SEC660 *Page 21*	FOR408 *Page 22*								
Cyber Defence Canberra Canberra • 27 Jun - 9 Jul		SEC401 *Page 9* WEEK 1	SEC501 *Page 10* WEEK 2	SEC503 *Page 11* WEEK 1	SEC504 *Page 12* WEEK 1			SEC550 *Page 15* WEEK 2	SEC560 *Page 16* WEEK 2		SEC573 *Page 19* WEEK 2				FOR508 *Page 23* WEEK 2				AUD507 *Page 29* WEEK 1	ICS410 *Page 31* WEEK 1		
Adelaide Adelaide • 5-10 Sep		SEC401 *Page 9*							SEC560 *Page 16*													
Sydney Sydney • 7-19 Nov	SEC301 *Page 8* WEEK 1	SEC401 *Page 9* WEEK 1			SEC504 *Page 12* WEEK 1	SEC511 *Page 13* WEEK 2	SEC542 *Page 14* WEEK 2									FOR572 *Page 25* WEEK 2	FOR578 *Page 26* WEEK 1	FOR610 *Page 28* WEEK 2			ICS515 *Page 32* WEEK 2	

SINGAPORE

	SEC401 Security Essentials Bootcamp Style	SEC501 Advanced Security Essentials – Enterprise Defender	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 Hackinge	SEC550 Active Defense, Offensive Countermeasures and Cyber Deception	SEC560 Network Penetration Testing and Ethical Hacking	SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	FOR408 Windows Forensic Analysis	FOR508 Advanced Digital Forensics and Incident Response	FOR572 Advanced Network Forensics and Analysis	FOR578 Cyber Threat Intelligence	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	AUD507 Auditing & Monitoring Networks, Perimeters, and Systems	ICS410 ICS/SCADA Security Essentials	ICS515 ICS Active Defense and Incident Response	MGT535 Incident Response Team Management
Secure Singapore Singapore • 28 Mar - 9 Apr				SEC504 *Page 12* WEEK 1	SEC511 *Page 13* WEEK 1	SEC542 *Page 14* WEEK 1	SEC550 *Page 15* WEEK 2		SEC566 *Page 18* WEEK 2			FOR408 *Page 22* WEEK 1			FOR578 *Page 26* WEEK 2	FOR610 *Page 28* WEEK 1	AUD507 *Page 29* WEEK 1		ICS515 *Page 32* WEEK 1	
SOS October Singapore Singapore • 24 Oct - 6 Nov	SEC401 *Page 9* WEEK 2	SEC501 *Page 10* WEEK 1	SEC503 *Page 11* WEEK 1	SEC504 *Page 12* WEEK 2				SEC560 *Page 16* WEEK 1		SEC575 *Page 20* WEEK 1	SEC660 *Page 21* WEEK 1		FOR508 *Page 23* WEEK 1	FOR572 *Page 25* WEEK 2				ICS410 *Page 31* WEEK 2		MGT535 *Page 32* WEEK 2

SANS ASIA-PACIFIC 2016 EVENT SCHEDULE

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

REGISTRATION: sans.org

CONTACT: AsiaPacific@sans.org
+65 69 339 540

INDIA

	SEC501 Advanced Security Essentials – Enterprise Defender	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	SEC542 Web App Penetration Testing and Ethical Hackinge	SEC560 Network Penetration Testing and Ethical Hacking	SEC561 Immersive Hands-On Hacking Techniques	SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	SEC575 Mobile Device Security and Ethical Hacking	FOR508 Advanced Digital Forensics and Incident Response	FOR518 Mac Forensic Analysis	FOR572 Advanced Network Forensics and Analysis	FOR585 Advanced Smartphone Forensics	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	AUD507 Auditing & Monitoring Networks, Perimeters, and Systems	DEV522 Defending Web Applications Security Essentials	ICS410 ICS/SCADA Security Essentials	ICS515 ICS Active Defense and Incident Response
Cyber Defense Delhi Delhi • 11-16 January							SEC566 *Page 18*						FOR610 *Page 28*				
Secure India Bangalore • 22 Feb - 5 Mar	SEC501 *Page 10* WEEK 1	SEC504 *Page 12* WEEK 1							FOR508 *Page 23* WEEK 2								ICS515 *Page 32* WEEK 2
DFIR Delhi Delhi • 25 July - 6 Aug									FOR508 *Page 23* WEEK 1		FOR572 *Page 25* WEEK 1	FOR585 *Page 27* WEEK 2					
Bangalore Bangalore • 19 Sep - 1 Oct			SEC511 *Page 13* WEEK 1		SEC560 *Page 16* WEEK 2			SEC575 *Page 20* WEEK 1		FOR518 *Page 24* WEEK 1				AUD507 *Page 29* WEEK 2			
Hyderabad Hyderabad • 28 Nov - 3 Dec				SEC542 *Page 14*		SEC561 *Page 17*									DEV522 *Page 30*	ICS410 *Page 31*	

JAPAN

	SEC401 Security Essentials Bootcamp Style	SEC503 Intrusion Detection In-Depth	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	SEC560 Network Penetration Testing and Ethical Hacking	SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	FOR508 Advanced Digital Forensics and Incident Response	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Secure Japan Tokyo • 15-20 Feb	SEC401 (In Japanese) *Page 9*	SEC503 *Page 11*	SEC504 *Page 12*		SEC560 *Page 15*			
Tokyo Autumn Tokyo • 17-29 Oct			SEC504 *Page 12* WEEK 1	SEC511 *Page 13* WEEK 1		SEC566 *Page 18* WEEK 2	FOR508 *Page 23* WEEK 2	FOR610 *Page 28* WEEK 2

PHILIPPINES

	SEC401 Security Essentials Bootcamp Style	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling
Philippines Makati, Metro Manila • 20-25 June	SEC401 *Page 9*	SEC504 *Page 12*

MALAYSIA

	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC560 Network Penetration Testing and Ethical Hacking
Community SANS APAC Kuala Lumpur • 8-13 Aug	SEC504 *Page 12*	SEC560 *Page 16*

WHO SHOULD ATTEND:

- People who are new to information security and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don't understand, but want to understand
- Non-IT security managers who worry their company will be the next mega-breach headline story on the 6 o'clock news
- Professionals in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification

SANS SEC301

TRAINING EVENTS:

Sydney
Sydney
7-11 Nov

NEW

SEC301
Intro to Information Security

Five-Day Program | 30 CPEs | Laptop Required

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

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

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

"I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful."
-Ron Hoffman, Mutual of Omaha

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

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

"I would recommend this course to anyone entering information security. I wish every security professional will be able to build the foundation of their career in security by taking SEC301! This was a basic review for me personally but good, solid information to newbies."
-Kimberly Hawkins, Scottrade

giac.org

sans.org/ondemand

SEC401
Security Essentials Bootcamp Style

Six-Day Program | 46 CPEs | Laptop Required

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

STOP and ask yourself the following questions:

- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

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

giac.org | sans.edu | sans.org/ondemand

WHO SHOULD ATTEND:

- Security professionals
- Managers
- Operations personnel
- IT engineers and supervisors
- Administrators
- Forensic specialists, penetration testers, and auditors

SANS SEC401

TRAINING EVENTS:

Secure Japan
(In Japanese)
Tokyo
2-24 Feb

Secure Canberra
Canberra
18-23 Apr

Philippines
Makati, Metro Manila
20-25 Jun

Cyber Defence Canberra
Canberra
27 Jun - 2 Jul

Adelaide
Adelaide
5-10 Sep

SOS October Singapore
Singapore
1-6 Nov

Sydney
Sydney
8-13 Nov

WHO SHOULD ATTEND:

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

SANS SEC501

TRAINING EVENTS:

Secure India
Bangalore
22-27 Feb

Cyber Defence Canberra
Canberra
4-9 Jul

SOS October Singapore
Singapore
24-29 Oct

SEC501
Advanced Security Essentials – Enterprise Defender

Six-Day Program | 36 CPEs | Laptop Required

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

"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

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

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

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

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

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

GIAC Certified Enterprise Defender GCED
giac.org

SANS Technology Institute
sans.edu

sans.org/ondemand

SEC503
Intrusion Detection In-Depth

Six-Day Program | 36 CPEs | Laptop Required

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

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

"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

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

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

"As usual, SANS courses pay for themselves by day two. By day three, you are itching to get back to the office to use what you've learned."
-Ken Evans, CSSC

giac.org | sans.edu | sans.org/ondemand

WHO SHOULD ATTEND:

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

SANS SEC503

TRAINING EVENTS:

Secure Japan
Tokyo • 15-20 Feb

Cyber Defence Canberra
Canberra
27 Jun - 2 Jul

SOS October Singapore
Singapore
24-29 Oct

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

SANS SEC504

TRAINING EVENTS:

Secure Japan
Tokyo
15-20 Feb

Secure India
Bangalore
22-27 Feb

Secure Singapore
Singapore
21-26 Mar

Philippines
Makati, Metro Manila
20-25 Jun

Cyber Defence Canberra
Canberra
27 Jun - 2 Jul

Community SANS
Kuala Lumpur
8-13 Aug

Tokyo Autumn
Tokyo
17-22 Oct

SOS October Singapore
Singapore
31 Oct - 5 Nov

Sydney
Sydney
7-12 Nov

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program | 37 CPEs | Laptop Required

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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

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

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

"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


sans.org/ondemand

SEC511
Continuous Monitoring and Security Operations

Six-Day Program | 36 CPEs | Laptop Required

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!

With your training journey now complete and your skills enhanced and honed, it is time to go back to work and deliver on the SANS promise that you will be able to apply what you learn in this course the day you return to the office.

giac.org | sans.edu | sans.org/ondemand

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)

SANS SEC511

TRAINING EVENTS:

Secure Singapore
Singapore
21-26 Mar

Melbourne
Melbourne
16-21 May

Bangalore
Bangalore
19-24 Sep

Tokyo Autumn
Tokyo
17-22 Oct

Sydney
Sydney
14-19 Nov

WHO SHOULD ATTEND:

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

SANS SEC542

TRAINING EVENTS:

Secure Singapore
Singapore
21-26 Mar

Sydney
Sydney
14-19 Nov

Hyderabad
Hyderabad
28 Nov - 3 Dec

SEC542
Web App Penetration Testing and Ethical Hacking

Six-Day Program | 36 CPEs | Laptop Required

Web applications play a vital role in every modern organization. But, if your organization doesn't properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way to hammer home lessons learned.

giac.org

sans.edu


sans.org/ondemand

NEW

SEC550
Active Defense, Offensive Countermeasures and Cyber Deception

Five-Day Program | 30 CPEs | Laptop Required

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

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

You Will Learn:

- How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker
- How to gain better attribution as to who is attacking you and why
- How to gain access to a bad guy's system
- Most importantly, you will find out how to do the above legally

Author Statement

TI wrote this course to finally make defense fun, to finally add some confusion to the attackers, and to change the way we all look at defense. One of the most frequent questions I get is why offensive countermeasures are so important. Many people tell me that we cannot ignore patching, firewalls, policies, and other security management techniques. I cannot agree more. The techniques presented in this course are intended for organizations that have gone through the process of doing things correctly and want to go further. Get your house in order, and then play. Of course, there will be challenges for anyone trying to implement offensive countermeasures in their organization. However, they can all be faced and overcome.
-John Strand

WHO SHOULD ATTEND:

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

SANS SEC550

TRAINING EVENTS:

Secure Singapore
Singapore
28 Mar - 1 Apr

Cyber Defence Canberra
Canberra
4-8 Jul

WHO SHOULD ATTEND:

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

SANS SEC560

TRAINING EVENTS:

Secure Japan
Tokyo
15-20 Feb

Cyber Defence Canberra
Canberra
4-9 Jul

Community SANS
Kuala Lumpur
8-13 Aug

Adelaide
Adelaide
5-10 Sep

Bangalore
Bangalore
26 Sep - 1 Oct

SOS October Singapore
Singapore
24-29 Oct

SEC560
Network Penetration Testing and Ethical Hacking

Six-Day Program | 37 CPEs | Laptop Required

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

"This type of training is fantastic, all new penetration testers and personnel who interact with testers or set up assessments should take SEC560." -Christopher Duffy, Knowledge Consulting Group

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

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

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

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

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

"I really enjoyed having real-world stories, not just technical 'how-to,' but also the logistical items such as cleaning up after the pen test."
-Matt Armstrong, Stroz Friedberg, LLC

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

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

giac.org | sans.edu | sans.org/ondemand

SEC561
Immersive Hands-On Hacking Techniques

Six-Day Program | 36 CPEs | Laptop Required

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

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

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

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

WHO SHOULD ATTEND:

- Security professionals
- Systems and network administrators
- Incident response analysts
- Forensic analysts
- Penetration testers

SANS
SEC561

TRAINING EVENTS:

Secure Canberra
Canberra
18-23 Apr

Hyderabad
Hyderabad
28 Nov - 3 Dec

WHO SHOULD ATTEND:

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

SANS
SEC566

TRAINING EVENTS:

Cyber Defense Delhi
Delhi
11-15 Jan

Secure Singapore
Singapore
28 Mar - 1 Apr

Tokyo Autumn
Tokyo
24-28 Oct

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

Five-Day Program | 30 CPEs | Laptop Required

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the 20 Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

"The instructor does an outstanding job of providing an overview of each control as well as offering his perspective and experience, which adds a lot of value." -Danny Tomlinson, Kapstone Paper

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

"This class is extremely valuable for any organization wanting to know where they stand on security." -David O'Brien, Costco

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. Specifically, by the end of the course students will know how to:

- **Create a strategy to successfully defend their data**
- **Implement controls to prevent data from being compromised**
- **Audit systems to ensure compliance with Critical Control standards.**

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

giac.org

sans.edu


sans.org/ondemand

REGISTRATION: sans.org CONTACT: AsiaPacific@sans.org | +65 69 339 540

SEC573
Python for Penetration Testers

Five-Day Program | 30 CPEs | Laptop Required

Your target has been well hardened. So far, your every attempt to compromise their network has failed. You did find evidence of vulnerability, a break in their defensive posture. Unfortunately, all of your tools have failed to successfully exploit it. Your employers demand results. You want to model the actions of an advanced adversary and take advantage of that discovered flaw your tools can't seem to address. What do you do when off-the-shelf tools fall short? You write your own tool!

SEC573: Python for Penetration Testers will teach you the skills needed not only to tweak or customize tools, but to even develop your own tools from scratch. The course is designed to meet you at your current skill level and appeal to a wide variety of backgrounds. Whether you have absolutely no coding experience or are a skilled Python developer looking to apply your coding skills to penetration testing, this course has something for you.

You cannot become a world-class tool builder by merely listening to lectures, so this course is chock full of hands-on labs. Every day we will teach you the skills you need to develop serious Python programs and show you how to apply those skills in penetration testing engagements.

The course begins with an introduction to SANS pyWars, which is a four-day Capture the Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own pace. Experienced programmers can quickly progress to more advanced concepts while novice programmers spend time building a strong foundation.

We then cover the essential skills required to get the most out of the Python language. The essentials workshop labs will teach you the concepts and techniques required to develop your own tools. The workshop focuses on essential programming skills and how to apply them in real-world scenarios, but it also shows you shortcuts that will make even experienced developers more deadly. Once everyone understands the essentials, we apply those skills by developing tools to help you in your next penetration test. You will develop a port-scanning, anti-virus-evading, client-infecting backdoor for placement on target systems, as well as a SQL injection tool to extract data from websites that are immune to off-the-shelf tools. You will learn the concepts required to build a multi-threaded password guessing tool and a packet assembling network reconnaissance tool. The course concludes with a capstone one-day Capture the Flag event that complements the pyWars challenge and tests your ability to apply your new tools and coding skills in a penetration testing challenge.

The ability to read, write, and customize software is what distinguishes the good penetration tester from the great one. The best penetration testers can customize existing open-source tools or develop their own tools. Unfortunately, even though organizations serious about security continually emphasize their need for skilled tool builders, many testers do not have these skills. Developing these skills is not beyond your reach. So when you are ready to fully weaponize your penetration testing skillset and build and use your own tools to automate your penetration testing skills, join us for SEC573: Python for Penetration Testers.

WHO SHOULD ATTEND:

- Security professionals who want to learn how to develop Python applications.
- Penetration testers who want to move from being a consumer of security tools to being a creator and customizer of security tools.
- Technologists who need custom tools to test their infrastructure and want to create those tools themselves.

SANS SEC573

TRAINING EVENTS:

Cyber Defence Canberra
Canberra
4-8 Jul

WHO SHOULD ATTEND:

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Red team members
- Blue team members

SANS SEC575

TRAINING EVENTS:

Secure Canberra
Canberra
18-23 Apr

Bangalore
Bangalore
19-24 Sep

SOS October Singapore
Singapore
24-29 Oct

SEC575
Mobile Device Security and Ethical Hacking

Six-Day Program | 36 CPEs | Laptop Required

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large 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 (ERP) to project management.

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

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **High probability of the device being hacked, lost or stolen**

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.

"SEC575 offers invaluable material. [The course instructor's] energy and enthusiasm are incomparable!"
-Randy Pauli, Chelan County PUD

You Will Learn:

- How to capture and evaluate mobile application network activity
- How to decrypt and manipulate Apple iOS application behavior
- How to identify the steps taken by Android malware
- How to reverse-engineer and change Android applications in the Google Play Store
- How to conduct mobile device and mobile application penetration tests

giac.org

sans.edu


sans.org/ondemand

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program | 46 CPEs | Laptop Required

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!

"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

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need 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 is actually a technical class and not 'fad' info security garbage everyone else is teaching."
-Kyle Hanslovan, ManTech

Among the biggest benefits of SEC660 is the expert-level hands-on guidance provided through the labs and the additional time allotted each evening to reinforce daytime material and master the exercises.

"The SEC660 course was hands-on, packed with content, and current to today's technology!"
-Michael Horken, Rockwell Automation

giac.org sans.edu sans.org/ondemand

WHO SHOULD ATTEND:

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

SANS SEC660

TRAINING EVENTS:

Melbourne
Melbourne
16-21 May

WHO SHOULD ATTEND:

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

SANS FOR408

TRAINING EVENTS:

Secure Singapore
Singapore
21-26 Mar

Melbourne
Melbourne
16-21 May

FOR408
Windows Forensic Analysis

Six-Day Program | 36 CPEs | Laptop Required

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

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

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 7, Windows 8/8.1, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 8.1 artifacts.

FOR408 is continually updated: This course utilizes a brand-new intellectual property theft and corporate espionage case that took over 6 months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator can encounter while analyzing Windows systems. The incredibly detailed workbook details the tools and techniques step-by-step that each investigator should follow to solve a forensic case.

MASTER WINDOWS FORENSICS –
YOU CAN'T PROTECT WHAT YOU DON'T UNDERSTAND

giac.org

sans.edu


sans.org/ondemand

digital-forensics.sans.org

REGISTRATION: sans.org CONTACT: AsiaPacific@sans.org | +65 69 339 540

FOR508
Advanced Digital Forensics and Incident Response

Six-Day Program | 36 CPEs | Laptop Required

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

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

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

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

"FOR508 is packed with outstanding in-depth information."
-Craig Goldsmith, OCRFL

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

"The SANS508 course exceeded my expectations in every way. it provided me the skills, knowledge, and tools to effectively respond to and handle APT's and other enterprise wide threats."
-Josh Moulin, NSTEC/NNSA/DOE

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

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

giac.org | sans.edu | sans.org/ondemand | digital-forensics.sans.org

WHO SHOULD ATTEND:

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

SANS FOR508

TRAINING EVENTS:

Secure India
Bangalore
29 Feb - 5 Mar

Cyber Defence Canberra
Canberra
4-9 Jul

DFIR Delhi
Delhi
25-30 Jul

Tokyo Autumn
Tokyo
24-29 Oct

SOS October Singapore
Singapore
24-29 Oct

WHO SHOULD ATTEND:

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

SANS
FOR518

TRAINING EVENTS:

Bangalore
Bangalore
19-24 Sep

NEW

FOR518
Mac Forensic Analysis

Six-Day Program | 36 CPEs | Laptop Required

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.

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

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.

FOR518: Mac Forensic Analysis will teach you:

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

"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.

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.

FORENSICATE DIFFERENTLY!

sans.org/ondemand

digital-forensics.sans.org

FOR572
Advanced Network Forensics and Analysis

Six-Day Program | 36 CPEs | Laptop Required

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. The course focuses on the knowledge necessary to expand the forensic mindset from residual data on the storage media of 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.***

"I research ICS/SCADA environments. I think FOR572 presents a better approach at detecting malware then a more traditional approach does."
-Niklas Vilhelm, Norwegian National Security Authority

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.

BAD GUYS ARE TALKING –
WE'LL TEACH YOU TO LISTEN

giac.org | sans.edu | sans.org/ondemand | digital-forensics.sans.org

WHO SHOULD ATTEND:

- Incident response team members and forensicators
- Security Operations Center (SOC) personnel and information security practitioners
- Network defenders
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network engineers
- Information technology professionals

SANS
FOR572

TRAINING EVENTS:

DFIR Delhi
Delhi
25-30 Jul

SOS October Singapore
Singapore
31 Oct - 5 Nov

Sydney
Sydney
14-19 Nov

WHO SHOULD ATTEND:

- Incident response team members
- Experienced digital forensic analysts
- Information security professionals
- Law enforcement officers, federal agents, or detectives
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

SANS FOR578

TRAINING EVENTS:

Secure Singapore
Singapore
28 Mar - 2 Apr

Sydney
Sydney
7-12 Nov

NEW

FOR578
Cyber Threat Intelligence

Five-Day Program | 30 CPEs | Laptop Required

Make no mistake: current computer network defense and incident response contain a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

FOR578: Cyber Threat Intelligence will help network defenders and incident responders determine:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions.

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578: Cyber Threat Intelligence will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

DFIR
digital-forensics.sans.org

FOR585
Advanced Smartphone Forensics

Six-Day Program | 36 CPEs | Laptop Required

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

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

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

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

"The topics covered in the course can be considered advanced but are also very practical. Topics such as parsing and searching devices not supported by commercial tools and digging in hex for deleted artifacts are extremely important."
-Matthew Edmondson

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

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU!

sans.org/ondemand

WHO SHOULD ATTEND:

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, or detectives
- IT auditors
- SANS SEC575, FOR408, FOR508, and FOR518 graduates looking to take their skills to the next level

SANS
FOR585

TRAINING EVENTS:

DFIR Delhi
Delhi
1-6 Aug

WHO SHOULD ATTEND:

- Incident responders
- Malware technologists
- Forensic investigators and IT practitioners

SANS
FOR610

TRAINING EVENTS:

Cyber Defense Delhi
Delhi
11-16 Jan

Secure Singapore
Singapore
21-26 Mar

Tokyo Autumn
Tokyo
24-29 Oct

Sydney
Sydney
14-19 Nov

FOR610
Reverse-Engineering Malware: Malware Analysis Tools & Techniques

Six-Day Program | 36 CPEs | Laptop Required

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

"FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats."
-Paul Gunnerson, U.S. Army

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to understand the inner workings of malicious software and uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. Additionally, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

This course will teach you how to handle self-defending malware, learning to bypass the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts and deobfuscating JavaScript and VBScript to understand the nature of the attack.

You will also learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if it exhibits rootkit characteristics.

The course culminates with a series of capture-the-flag challenges designed to reinforce the techniques learned in class and that provide additional opportunities to learn practical malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

giac.org

sans.edu


sans.org/ondemand

digital-forensics.sans.org

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program | 36 CPEs | Laptop Required

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

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

This course is specifically organized 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 that these controls address. 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.

"In 20+ years of industry experience, I have never seen a smoother intro to batch progress to branching and looping. Well done!"
-Michael Decker, CNS Security

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 theory, hands-on exercises, 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 auditors 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

SANS AUD507

TRAINING EVENTS:

Secure Singapore
Singapore
21-26 Mar

Cyber Defence Canberra
Canberra
27 Jun - 2 Jul

Bangalore
Bangalore
26 Sep - 1 Oct

giac.org | sans.edu | sans.org/ondemand | digital-forensics.sans.org

WHO SHOULD ATTEND:

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

SANS
DEV522

TRAINING EVENTS:

Hyderabad
Hyderabad
28 Nov - 3 Dec

DEV522
Defending Web Applications Security Essentials

Six-Day Program | 36 CPEs | Laptop Required

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

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

"As the world moves everything online, DEV522 is a necessity."
-Chris Spinder, B/E Aerospace, Inc.

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

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

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

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

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

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

giac.org | sans.edu | sans.org/ondemand

ICS410
ICS/SCADA Security Essentials

Five-Day Program | 30 CPEs | Laptop Required

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.

"This course was a good intro to ICS and provided simple ways to secure your network. It also gives an awareness to a number of avenues of attack. -Justin Mullins, DoD

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

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

giac.org

sans.org/ondemand

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

SANS ICS410

TRAINING EVENTS:

Cyber Defence Canberra
Canberra
27 Jun - 1 Jul

SOS October Singapore
Singapore
31 Oct - 4 Nov

Hyderabad
Hyderabad
28 Nov - 2 Dec

WHO SHOULD ATTEND:

- IT and OT Support
- IT and OT Cybersecurity
- ICS Engineers

SANS ICS515

TRAINING EVENTS:

Secure India
Bangalore
29 Feb - 4 Mar

Secure Singapore
Singapore
21-25 Mar

Sydney
Sydney
14-18 Nov

NEW

ICS515
ICS Active Defense and Incident Response

Five-Day Program | 30 CPEs | Laptop Required

Course Author - Robert M. Lee - This course is designed to empower students with the ability to understand and utilize active defense mechanisms in concert with incident response for industrial control system networks to respond to and deny cyber threats. This class uses a hands-on approach to give students a technical understanding of concepts such as generating and using threat intelligence, communicating control system needs to information technology personnel to deploy appropriate defenses, detecting malicious actors or threats on control system networks, and performing threat triage and incident response to ensure the safety and reliability of operations technology.

Author Statement

In taking this course you will leave with the skills to identify and understand your networked infrastructure, monitor it for advanced threats, quickly respond to identified threats while keeping operations running, and extract lessons learned from interactions with the adversary to incorporate in your team's defense efforts or share with others in the form of threat intelligence.
-Robert M. Lee

WHO SHOULD ATTEND:

- Information security engineers and managers
- IT managers
- Operations managers
- Risk management professionals
- IT/system administration/ network administration professionals
- IT auditors

Business continuity and disaster recovery staff

SANS MGT535

TRAINING EVENTS:

SOS October Singapore
Singapore
31 Oct - 1 Nov

NEW

MGT535
Incident Response Team Management

Two-Day Program | 12 CPEs | Laptop Required

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense.

Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

This course was originally developed by Dr. Eugene Schultz, the founder of the first U.S. government incident response team and an information security professional with over 26 years of experience. The course has been updated to address current issues such as advanced persistent threat, incident response in the cloud, and threat intelligence.

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program | 33 CPEs | Laptop NOT Needed

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to *manage* security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

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

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

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

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class which aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

giac.org | sans.edu | sans.org/ondemand

WHO SHOULD ATTEND:

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

SANS MGT512

TRAINING EVENTS:

Secure Canberra
Canberra
18-23 Apr

ABOUT SANS

SANS is the most trusted and by far the largest source for information security training and security certification in the world.

The SANS Institute was established in 1989 as a cooperative research and education organization. Our training programs now reach more than 200,000 security professionals around the world.

SANS provides intensive immersion training, designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

SANS courses are full of important and immediately useful techniques that you can put to work as soon as you return to the office. They were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals. These courses address security fundamentals and awareness as well as the in-depth technical aspects of the most critical areas of IT security.

SANS certified instructors are recognized as the best in the world and are known for their unique blend of deep technical skill and teaching capability. To find the best teachers for each topic, SANS runs a continuous competition for instructors. The success rate to become a SANS certified instructor is approximately 1 out of 900 potential candidates.

SANS provides training through several delivery methods, both live and virtual classroom-style at a training event, online at your own pace, guided self-study with a local mentor, or private classes at your own workplace.

In addition to top-notch training, SANS offers certification through the GIAC security certification program and numerous free security resources such as newsletters, white papers, and webcasts.

Why SANS is the best training and educational investment

- Intensive, hands-on immersion training with the highest-quality courseware in the industry
- Incomparable instructors and authors who are industry experts and practitioners fighting the same cyber battles as you and discovering new ways to thwart attacks
- Training that strengthens a student's ability to achieve a GIAC certification, which is unique in the field of information security certifications because, it not only tests a candidate's knowledge, but also the candidate's ability to put the knowledge into practice in the real world

How to register for SANS training

The most popular option for taking SANS training is to attend a training event. SANS runs public training events in Australia, India, Japan, and Singapore (and globally) offering students the opportunity to take a SANS course across an intensive 5 or 6 days. SANS training events provide the perfect learning environment and offer the chance to network with other security professionals as well as SANS instructors and staff.

Students should register online by visiting www.sans.org or you can contact us at AsiaPacific@sans.org for further information.

SANS