THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS

2017 ASIA-PACIFIC
Course Catalog

AUSTRALIA INDIA JAPAN 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
www.sans.org

CONTACT US AT
AsiaPacific@sans.org
+65 6933 9540

GIAC
CERTIFICATIONS
GIAC-Approved Training

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

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

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

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

sans.org/community

Private Training

Your Location! Your Schedule!

sans.org/private-training

Mentor

Live Multi-Week Training with a Mentor

sans.org/mentor

Summit

Live IT Security Summits and Training

sans.org/summit

ONLINE TRAINING

OnDemand

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

sans.org/ondemand

vLive

Online, Evening Courses with SANS' Top Instructors

sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

sans.org/simulcast

OnDemand Bundles

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

Dear Colleague,


Suresh Mustapha

We are pleased to share the updated 2017 SANS Asia Pacific course catalogue with you. Thanks to the ongoing support of the Asia Pacific Information Security Community, we are able to expand our regional offering to provide a wider range of our introductory, intermediate, and advanced information security and digital forensics courses at several new locations. Our 2017 program features new events in Adelaide and Tokyo, in addition to a broader selection of cutting-edge courses at our core regional events.

Please review this catalogue with your colleagues and start making plans to attend the relevant classes at the times and locations most convenient to you and your team. And if there is something you believe we should consider adding to the program, please reach out to us at **AsiaPacific@sans.org** and we'll see what can be done to accommodate your organization's needs.

Some of the exciting new courses in our 2017 roster include:

MGT517: Managing Security Operations. (5 days) There are a large number of companies trying to figure out what a SOC is, and how to establish one. This course entails the design, build, operation, and ongoing growth of all facets of the security capability of the organization, including: establishing the Security Operations Program governance; designing and developing the SOC; hiring and cultivating staff; ongoing operations of network security monitoring, threat intelligence, incident response, forensics, and self-assessment through vulnerability scanning and penetration testing.

SEC567: Social Engineering for Penetration Testers. (2 days) This new short course provides the blend of knowledge required to add social engineering skills to your Penetration Testing portfolio. Successful social engineering utilizes psychological principles and technical techniques to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychology foundations required to craft effective attacks and bolsters this with many examples of what works from both cyber criminals and the authors experience in engagements. On top of these principles we provide a number of tools (produced in our engagements over the years and now available in the course) and also labs centered on the key technical skills required to measure your social engineering success and report it to your company or client.

Hosted: Health Care Security Essentials. (2 days) Health Care Security Essentials is designed to provide SANS students with an introduction to current and emerging issues in health care information security and regulatory compliance. The goal of this course is to present a substantive overview and analysis of relevant information security subject matter that is having a direct and material impact on health care systems globally. The class provides a foundational set of skills and knowledge for health care security professionals by integrating case studies, hands-on labs, and tips for securing and monitoring electronic Protected Health Information (ePHI).

Kindest regards,

Suresh Mustapha
MD Asia Pacific

Training Roadmap | **Choose Your Path**

Baseline Skills

1 You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the "offense informs defense" preparation teaching defense specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC504.

- SEC**401** Security Essentials Bootcamp Style — **GSEC** Certification Security Essentials
- SEC**504** Hacker Tools, Techniques, Exploits and, Incident Handling — **GCIH** Certification Certified Incident Handler

1b You will be responsible for managing security teams or implementations, but do not require hands-on skills

Security Management

- MGT**512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ — **GSLC** Certification Security Leadership
- SEC**566** Implementing and Auditing the Critical Security Controls-In-Depth — **GCCC** Certification Critical Security Controls

New to Cybersecurity?

- SEC**301** — **GISP** Certification

Intermediate Job Roles

2 You are experienced in security, preparing for a specialized job role or focus

Security Monitoring and Detection

- SEC**503** Intrusion Detection In-Depth — **GCIA** Certification Certified Intrusion Analyst
- SEC**511** Continuous Monitoring and Security Operations — **GMON** Certification Continuous Monitoring

Penetration Testing & Vulnerability Analysis

- SEC**560** Network Penetration Testing and Ethical Hacking — **GPEN** Certification Penetration Tester
- SEC**542** Web App Penetration Testing and Ethical Hacking — **GWAPT** Certification Web Application Penetration Tester

Incident Response and Enterprise Forensics

- FOR**508** Advanced Digital Forensics, Incident Response, and Threat Hunting — **GCFA** Certification Forensic Analyst
- FOR**572** Advanced Network Forensics and Analysis — **GNFA** Certification Network Forensic Analyst

- MGT**414** SANS Training Program for CISSP® Certification — **GISP** Certification Information Security Professional

Crucial Skills, Specialized Roles

SANS' comprehensive catalog enables professionals to deepen their technical skills in key practice areas. It also directly addresses other audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 You are a candidate for specialized or advanced training

Cyber Defense Operations

- SEC**501** Advanced Security Essentials – Enterprise Defender **GCED**
- SEC**505** Securing Windows and PowerShell Automation **GCWN**
- SEC**506** Securing Linux/Unix | **GCUX**
- SEC**579** Virtualization and Software-Defined Security

Industrial Control Systems Security

- ICS**410** ICS/SCADA Security Essentials | **GICSP**
- ICS**456** Essentials for NERC Critical Infrastructure Protection
- ICS**515** ICS Active Defense and Incident Response

Penetration Testing and Ethical Hacking

- SEC**550** Active Defense, Offensive Countermeasures and Cyber Deception
- SEC**561** Immersive Hands-On Hacking Techniques
- SEC**562** CyberCity Hands-on Kinetic Cyber Range Exercise
- SEC**573** Automating Information Security for Python **GPYC**
- SEC**575** Mobile Device Security and Ethical Hacking **GMOB**
- SEC**617** Wireless Ethical Hacking, Penetration Testing, and Defenses | **GAWN**
- SEC**642** Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
- SEC**660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN**
- SEC**760** Advanced Exploit Development for Penetration Testers

Digital Forensics and Incident Response

- FOR**408** Windows Forensic Analysis | **GCFE**
- FOR**518** Mac Forensic Analysis
- FOR**526** Memory Forensics In-Depth
- FOR**578** Cyber Threat Intelligence
- FOR**585** Advanced Smartphone Forensics | **GASF**
- FOR**610** Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM**

Software Security

- DEV**522** Defending Web Applications Security Essentials | **GWEB**
- DEV**541** Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA**
- DEV**544** Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET**

Management

- MGT**514** IT Security Strategic Planning, Policy, and Leadership
- MGT**517** Managing Security Operations: Detection, Response, and Intelligence
- MGT**525** IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM**

Audit | Legal

- AUD**507** Auditing & Monitoring Networks, Perimeters, and Systems | **GSNA**
- LEG**523** Law of Data Security and Investigations | **GLEG**

SANS 2017 EVENT SCHEDULE

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

AUSTRALIA

	SEC301 Intro to Information Security	SEC401 Security Essentials Bootcamp Style	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC505 Securing Windows and PowerShell Automation	SEC511 Continuous Monitoring and Security Operations	SEC542 Web App Penetration Testing and Ethical Hacking	SEC550 Active Defense, Offensive Countermeasures and Cyber Deception	SEC560 Network Penetration Testing and Ethical Hacking	SEC573 Automating Information Security with Python	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting	FOR578 Cyber Threat Intelligence	MGT433 Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program	Core NetWars TOURNAMENT
Secure Canberra Canberra • 13-25 Mar		SEC401	SEC504		SEC511					SEC575	SEC660			MGT433	
Melbourne Melbourne • 22-27 May		SEC401				SEC542	SEC550					FOR508			
Cyber Defence Canberra Canberra • 26 Jun - 8 Jul	SEC301 WEEK 1	SEC401 WEEK 2	SEC504 WEEK 2	SEC505 WEEK 1				SEC560 WEEK 1	SEC573 WEEK 2				FOR578 WEEK 1		Core NetWars WEEK 1

	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	FOR408 Windows Forensic Analysis	FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting	FOR572 Advanced Network Forensics and Analysis	FOR585 Advanced Smartphone Forensics	FOR610 REM: Malware Analysis Tools and Techniques	ICS410 ICS/SCADA Security Essentials	AUD507 Auditing & Monitoring Networks, Perimeters, and Systems	DFIR NetWars TOURNAMENT
Adelaide Adelaide • 21-26 Aug	SEC401	SEC503	SEC504			FOR408							
Sydney Sydney • 13-25 Nov	SEC401 WEEK 1		SEC504 WEEK 1	SEC511 WEEK 1	SEC560 WEEK 2		FOR508 WEEK 1	FOR572 WEEK 2	FOR585 WEEK 2	FOR610 WEEK 2	ICS410 WEEK 1	AUD507 WEEK 1	DFIR NetWars WEEK 1

SINGAPORE

	SEC301 Intro to Information Security	SEC401 Security Essentials Bootcamp Style	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	SEC542 Web App Penetration Testing and Ethical Hacking	SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	SEC760 Advanced Exploit Development for Penetration Testers	FOR408 Windows Forensic Analysis	FOR578 Cyber Threat Intelligence	FOR585 Advanced Smartphone Forensics	FOR610 REM: Malware Analysis Tools and Techniques	HOSTED Health Care Security Essentials **NEW!**	DFIR NetWars TOURNAMENT
Secure Singapore Singapore • 13-25 Mar	SEC301 WEEK 1	SEC401 WEEK 1	SEC504 WEEK 1	SEC511 WEEK 1	SEC542 WEEK 1	SEC566 WEEK 2	SEC760 WEEK 2	FOR408 WEEK 1	FOR578 WEEK 2	FOR585 WEEK 2	FOR610 WEEK 1	HOSTED WEEK 1	DFIR NetWars WEEK 2

	SEC401 Security Essentials Bootcamp Style	SEC501 Advanced Security Essentials – Enterprise Defender	SEC503 Intrusion Detection In-Depth	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC550 Active Defense, Offensive Countermeasures and Cyber Deception	SEC560 Network Penetration Testing and Ethical Hacking	SEC567 Social Engineering for Penetration Testers **NEW!**	SEC575 Mobile Device Security and Ethical Hacking	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting	FOR572 Advanced Network Forensics and Analysis	ICS410 ICS/SCADA Security Essentials	MGT517 Managing Security Operations: Detection, Response, and Intelligence	Core NetWars TOURNAMENT
Cyber Defence Singapore Singapore • 10-15 Jul	SEC401			SEC504		SEC560				FOR508				
SOS October Singapore Singapore • 16-28 Oct	SEC401 WEEK 1	SEC501 WEEK 2	SEC503 WEEK 1	SEC504 WEEK 1	SEC550 WEEK 2	SEC560 WEEK 2	SEC567 WEEK 2	SEC575 WEEK 1	SEC660 WEEK 1	FOR508 WEEK 1	FOR572 WEEK 1	ICS410 WEEK 2	MGT517 WEEK 2	Core NetWars WEEK 1

SANS 2017 EVENT SCHEDULE

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

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	SEC542 Web App Penetration Testing and Ethical Hacking	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, Incident Response, and Threat Hunting	FOR572 Advanced Network Forensics and Analysis	FOR578 Cyber Threat Intelligence	FOR610 REM: Malware Analysis Tools and Techniques	Core NetWars TOURNAMENT
Secure Japan Tokyo • 13-25 Feb	SEC401 JAPANESE WEEK 1	SEC503 WEEK 2	SEC504 JAPANESE WEEK 2			SEC560 WEEK 1				FOR408 WEEK 1	FOR508 WEEK 2				
Cyber Defence Japan Tokyo • 10-15 July	SEC401 JAPANESE		SEC504					SEC575	SEC660						Core NetWars
Tokyo Autumn Tokyo • 16-28 Oct	SEC401 JAPANESE WEEK 1		SEC504 JAPANESE WEEK 2	SEC511 WEEK 1	SEC542 WEEK 1	SEC560 WEEK 2	SEC566 WEEK 2				FOR508 WEEK 1	FOR572 WEEK 2	FOR578 WEEK 2	FOR610 WEEK 1	

INDIA	SEC401 Security Essentials Bootcamp Style	SEC503 Intrusion Detection In-Depth	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC511 Continuous Monitoring and Security Operations	SEC560 Network Penetration Testing and Ethical Hacking	FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting	FOR578 Cyber Threat Intelligence
Secure India Bangalore • 20 Feb - 4 Mar		SEC503 WEEK 2	SEC504 WEEK 1			FOR508 WEEK 1	FOR578 WEEK 2
Hyderabad Hyderabad • 7-12 Aug				SEC511	SEC560		
Bangalore Bangalore • 4-9 Dec	SEC401		SEC504				

PHILIPPINES	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling
Philippines Manila • 19-24 June	SEC504

SANS SEC301

Intro to Information Security

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

Secure Singapore
13-17 March

Cyber Defence Canberra
26-30 June

www.giac.org/gisf

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

"SEC301 is the perfect blend of technical and practical information for someone new to the field, would recommend to friend!"

-Steve Mecco, Draper

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

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

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp Style**. 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.***

Author Statement

If you want to be good at something, whether it be sports, music, science, math, or information security, you MUST have a solid grasp of the fundamentals. In fact, the better you understand the fundamentals the better you will be at a particular skillset. Without that foundation to build on, it is almost impossible to become a master at something. The Introduction to Information Security course is all about building those fundamentals and creating that foundation.

One of the things I enjoy most is seeing a student have that "ah-ha" moment. The moment when they suddenly understand a topic for the first time - often a topic they have wondered about for years. You can almost literally see the "light-bulb" of understanding appear over their head. There are "ah-ha" moments at every turn and on every day of the SEC301: Introduction to Information Security course.

- Keith Palmgren

Security Essentials Bootcamp Style

SANS SEC401

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.

"This was my first SANS course – I didn't know what to expect. Now that I've been through a course, I must say, the experience was fantastic!" -Gary Hughes, Seagate Technology

www.giac.org/gsec

www.sans.edu

www.sans.org/ondemand

TRAINING EVENTS

Secure Japan (Japanese)
Tokyo | 13-18 February

Secure Singapore
13-18 March

Secure Canberra
20-25 March

Melbourne
22-27 May

Cyber Defence Canberra
3-8 July

Cyber Defence Singapore
10-15 July

Cyber Defence Japan (Japanese)
10-15 July

Adelaide
21-26 August

SOS October Singapore
16-21 October

Tokyo Autumn (Japanese)
16-21 October

Sydney
13-18 November

Bangalore
4-9 December

Who Should Attend

- Security professionals
- Managers
- Operations personnel
- IT engineers and supervisors
- Administrators
- Forensic specialists, penetration testers, and auditors
- Anyone new to information security with some background in information systems and networking

SANS SEC501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

SOS October Singapore
23-28 October

www.giac.org/gced

www.sans.edu

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

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

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

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

"Paul is a great instructor with the ability to tie real-world threats to theory and practice." -Bruce Henkel, Harris Corp.

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.

"SEC501 is the perfect course to immerse enterprise security staff into essential skills. Failing to attend this course is done at the peril of your organization." -John N. Johnson, Houston Police Department

Author Statement

After one recent class, a student ran up and gave me a big hug (he was a retired football player, so I did not argue) and said, "SANS is awesome. I have been frustrated in my job for over a year and had lost hope that you really could secure an organization and that anything I did made a difference. Just as my light of hope was burning out, I decided to take the Security Essentials course, figuring it was a lost cause. After this class the fire is burning brighter than it ever was. I feel like a kid again and cannot wait to go back to my company and make a difference. However, I think my boss is scared because I called him eight times throughout the week, telling him all of the great information and practical knowledge I learned!"

Having taught thousands of students, I am confident you will be just as excited and get similar results from SEC501. However, just for reference, hugs are optional.

-Eric Cole

Intrusion Detection In-Depth

SANS SEC503

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?

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 sometimes 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 with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

"Today has been brilliant, bringing all of our skills together to achieve the challenge. I wish we could do this every day!" -Hayley Roberts, MOD

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 DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. 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.

Author Statement

When I was invited to be a member of a computer incident response team in the late 1990s (just after Al Gore invented the Internet), there was no formal cybersecurity training available. Consequently, I learned on the job and made my share, and then some, of mistakes. I was so naive that I tried to report an attack on our network by a host with an IP address in the 192.168 reserved private network, available for use by anyone. Needless to say, I got a very embarrassing enlightenment when someone clued me in. With the benefit of experience and the passage of time, there are many lessons to be shared with you. This knowledge affords you the opportunity to learn and practice in the classroom to prepare you for the fast-paced always-interesting job of intrusion detection analysts.

-Judy Novak

TRAINING EVENTS

Secure Japan
Tokyo | 20-25 February

Secure India
Bangalore | 27 Feb - 4 March

Adelaide
21-26 August

SOS October Singapore
16-21 October

GCIA
www.giac.org/gcia

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

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

SANS SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
37 CPEs
Laptop Required

TRAINING EVENTS

Secure Japan (Japanese)
Tokyo | 20-25 February

Secure India
Bangalore | 20-25 February

Secure Singapore
13-18 March

Secure Canberra
20-25 March

Philippines
Manila | 19-24 June

Cyber Defence Canberra
3-8 July

Cyber Defence Singapore
10-15 July

Cyber Defence Japan
10-15 July

Adelaide
21-26 August

SOS October Singapore
16-21 October

Tokyo Autumn (Japanese)
23-28 October

Sydney
13-18 November

Bangalore
4-9 December

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.

"Our organization has incident response pieces all over. This course is valuable in putting the pieces together and improving the plan and, more importantly, the mindset." -Tyler Burwitz, TEEX

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 for, 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, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

"Excellent course. I've learned about the techniques and tools used by the bad guys and I have a greater understanding of how to protect our network." -Howard Duck, Schools Financial Credit Union

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

Who Should Attend

- Incident handlers
- 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

www.giac.org/gcih

www.sans.edu

www.sans.org/ondemand

Securing Windows and PowerShell Automation

SANS SEC505

Six-Day Program
36 CPEs
Laptop Required

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – now what? A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we'll never win, and we'll never get ahead of the game. By the time your Security Information and Event Manager (SIEM) or monitoring system tells you a Domain Admin account has been compromised, IT'S TOO LATE.

For the assume breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

"On day one, I am already seeing ways to use this training at my job."
-Nick Papa, Chemical Bank

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. PowerShell is free and open-source on GitHub for Linux and Mac OS, too.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too. Besides, PowerShell is also simply fun to use.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don't cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and agile Windows security at the same time!

"Really great course for anyone involved in the administration or securing of windows environments." -David Hazar, Oracle

TRAINING EVENTS

Cyber Defence Canberra
26 June - 1 July

www.giac.org/gcwn

www.sans.edu

www.sans.org/ondemand

Who Should Attend

- Security Operations engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure or smart cards
- Anyone who needs to reduce malware infections

SANS SEC511

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Secure Singapore
13-18 March

Secure Canberra
20-25 March

Hyderabad
7-12 August

Tokyo Autumn
16-21 October

Sydney
13-18 November

www.giac.org/gmon

www.sans.edu

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

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

Who Should Attend

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

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant 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.

"I run SOCs and this course provides a gut check against what we are doing today." -Tim Housman, General Dynamics IT

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 this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

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!

Web App Penetration Testing and Ethical Hacking

SANS SEC542

Six-Day Program
36 CPEs
Laptop Required

Web applications play a vital role in every modern organization. However, 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.

"Everything is very well thought out and organized. The URLs used for the labs work flawlessly. Course content and teaching skills are great."
-Stephan Hofacker, InfoTrust AG

SEC542 helps students move beyond push-button scanning to professional, thorough, and 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. 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.

TRAINING EVENTS

Secure Singapore
13-18 March

Melbourne
22-27 May

Tokyo Autumn
16-21 October

www.giac.org/gwapt

www.sans.edu


Bundle OnDemand
with this course
www.sans.org/ondemand

"The content in SEC542 is very relevant as it features recently discovered vulnerabilities.."
-Malcolm King, Morgan Stanley

Who Should Attend

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

SANS SEC550

Active Defense, Offensive Countermeasures and Cyber Deception

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

Melbourne
22-26 May

SOS October Singapore
23-27 October

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.

Who Should Attend

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

You Will Be Able To

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

Course Author Statement

I 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

Network Penetration Testing and Ethical Hacking

SANS SEC560

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.

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

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently…and masterfully.

"This course has a direct correlation to my job duties, and the insight and use of various tools will make it a lot easier. You will learn some of the ways your systems are vulnerable." -Roland T., USAF

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

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

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

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

"I learned more in one class then in years of self study!"
-Bradley Milhorn, Compucom Inc.

TRAINING EVENTS

Secure Japan
Tokyo | 13-18 February

Cyber Defence Canberra
26 June - 1 July

Cyber Defence Singapore
26 June - 1 July

Hyderabad
7-12 August

SOS October Singapore
23-28 October

Tokyo Autumn
16-21 October

Sydney
20-25 November

www.giac.org/gpen

www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

SANS SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

Secure Singapore
20-24 March

Tokyo Autumn
16-20 October

www.giac.org/gccc

www.sans.edu

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

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- 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

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? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

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 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.

"This is a must-do course if you are looking to steer your company through some hefty controls to security." -Jeff Evenson, AgStar Financial Services

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

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

"I'm leaving the class with a great mindset aimed at evaluating the current environment and controls. SEC566 was good information with a great instructor!"
-Tom Kozelsky, Nexeo Solution

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

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

"I will be recommending that our whole security team take this course."
-Matthew Morris, DHS/OBIM

Social Engineering for Penetration Testers

SANS SEC567

NEW!

Two-Day Program
12 CPEs
Laptop Required

TRAINING EVENTS

SOS October Singapore
23-24 October

SEC567: Social Engineering for Penetration Testers provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical methods to measure your success and manage the risk. **SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks and bolsters this with many examples of what works taken from the experiences of both cyber criminals and the authors.** On top of these principles, the course offers a number of tools (produced during the authors' engagements over the years and now available in the course) and labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

You'll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You'll also learn how to conduct pretexting exercises, and we wrap up the course with a fun "Capture the Human" exercise to put what you've learned into practice. This is the perfect course to open up new attack possibilities, better understand the human vulnerability in attacks, and let you practice snares that have proven themselves in tests time and time again.

On day one of the course, we introduce you to key social engineering concepts, the goals of social engineering and a myriad of reconnaissance tools that will help prepare you for successful campaigns. We complete the day with exercises centered around the most popular and scalable form of social engineering, phishing. Each section includes how to execute the attack, what works and what doesn't and how to report on it to help the organization improve their defenses.

On day two, we build on the principles covered on day one of the course to focus heavily on payloads for your social engineering engagements. We will cover how to avoid detection, limit the risk of your payloads causing issues and how to build a bespoke payload that works and looks the part of your selected snare. Following that we will introduce another powerful skill with pretexting and cover how these can be combined to get payloads running. We end the day with a capture the flag where students can apply their new found skills and a section covering the top dos and don'ts in an engagement.

Course Author Statement

Social engineering has always been a critical part of the cyber criminals' toolkit and has been at the core of innumerable attacks over the years. Social engineering as part of penetration testing has become a massive interest of organizations and yet many penetration testers do not have it as part of their attack toolkit. We are passionate about changing that and opening up a new set of attack possibilities. That being said, this is an area filled with ethical challenges, risks, and even legal landmines and we've done our best to share our experiences in the course so people can reap the benefits of our experiences without falling in to the pitfalls we have over the years.
-James Lyne and Dave Shackleford

You Will Be Able To:

- Take on your first social engineering test in your company, or as a consultant
- Improve your social engineering know-how to develop new variations or increase your snare rate
- Equip you to deal with some of the ethical and risk challenges associated with social engineering engagements
- Enhance other penetration testing disciplines through understanding human behavior and how to exploit it

Who Should Attend

- Staff or consultant penetration testers looking to increase their test breadth and effectiveness
- Security defenders looking to enhance their understanding of attack techniques to improve their defenses
- Staff responsible for security awareness and education campaigns who want to understand how cyber criminals persuade their way through their defenses

SANS SEC573

Automating Information Security with Python

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Cyber Defence Canberra
3-8 July

www.giac.org/gpyc

www.sans.edu

"Excellent class for beginners and advanced alike. It has something for everyone."
-Mike Perez, Disney

"Best class ever! After just 2 days I'm getting comfortable with the nuances of Python. I never thought that would happen."
-Jay Wilson, Navient

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 the creator of security tools
- Technologists who need custom tools to test their infrastructure and who want to create those tools themselves

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold… or you can write a tool yourself.

Or, perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Or, as a Penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, **SEC573: Automating Information Security with Python** will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today's information security professional, and achieving more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

"SEC573 gave me exposure to tools and techniques I wouldn't have normally considered, but now are part of my arsenal." -Allen C., DoD

Mobile Device Security and Ethical Hacking

SANS SEC575

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Secure Canberra
20-25 March

Cyber Defence Japan
10-15 July

SOS October Singapore
16-21 October

"Taking this course was a great opportunity to ask an expert all my questions, good broad overview and mobile threats background!"
-Tom G., GovCert UK

www.giac.org/gmob

www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

Who Should Attend

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

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don't need to imagine any further because this already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

SANS SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Secure Canberra
20-25 March

Cyber Defence Japan
10-15 July

SOS October Singapore
16-21 October

www.giac.org/gxpn

www.sans.edu

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

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

Who Should Attend

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

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!

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 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

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

Advanced Exploit Development for Penetration Testers

SANS SEC760

Six-Day Program
46 CPEs
Laptop Required

TRAINING EVENTS

Secure Singapore
20-25 March

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

"SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned."
-Jenny Kitaichit, Intel

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

"No one can teach the material as clearly as Steve does. He is awesome." Wally Strzelec, Texas A&M University

Not sure if you are ready for SEC760?

Take this 10 question quiz:
www.sans.org/sec760/quiz

Who Should Attend

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

Author Statement

As a perpetual student of information security, I am excited to offer SEC760: Advanced Exploit Writing for Penetration Testers. Exploit development is a hot topic as of late and will continue to increase in importance moving forward. With all of the modern exploit mitigation controls offered by operating systems such as Windows 7 and 8, the number of experts with the skills to produce working exploits is highly limited. More and more companies are looking to hire professionals with the ability to conduct a Secure-SDLC process, perform threat modeling, determine if vulnerabilities are exploitable, and carry out security research. This course was written to help you get into these highly sought-after positions and to teach you cutting-edge tricks to thoroughly evaluate a target, providing you with the skills to improve your exploit development.
-Stephen Sims

SANS FOR408

Windows Forensic Analysis

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Secure Japan
Tokyo | 13-18 February

Secure Singapore
13-18 March

Adelaide
21-26 August

www.giac.org/gcfe

www.sans.edu

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

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

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

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.

"I have been doing forensic investigations for several years, but would highly recommend this course (FOR408) for both new and old forensic investigations." -Robert Galarza, JP Morgan Chase

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.

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 7/8/10, 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 10 artifacts.

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

FOR408 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six 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 might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook details the tools and techniques that each investigator should follow to solve a forensic case.

Advanced Digital Forensics, Incident Response, and Threat Hunting

SANS FOR508

Six-Day Program
36 CPEs
Laptop Required

FOR508: Advanced Digital Forensics, Incident Response, and Theat Hunting will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

"This was a great course. I learned some great techniques and this will lead to some changes in our incident response process." -Rick, Syngenta

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

"So far this is the best course I've taken in 20 years."
-Mauricio Bellido Jr., USG

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

TRAINING EVENTS

Secure Japan
Tokyo | 20-25 February

Secure India
Bangalore | 20-25 February

Melbourne
22-27 May

Cyber Defence Singapore
10-15 July

SOS October Singapore
16-21 October

Tokyo Autumn
16-21 October

Sydney
13-18 November

Who Should Attend

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

GCFA
www.giac.org/gcfa

SANS Technology Institute
www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

SANS FOR572

Advanced Network Forensics and Analysis

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

SOS October Singapore
16-21 October

Tokyo Autumn
16-21 October

Sydney
20-25 November

www.giac.org/gnfa

www.sans.edu

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

Who Should Attend

- Incident response team members and forensicators
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

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 overlookingthe network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

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

"FOR572 was an excellent course that kept my attention and it will be immediately useful when I get back to work." -John Ives, UC Berkeley

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

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cyber crime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpxtract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy to make easy work of ripping through hundreds and thousands of data records.

Cyber Threat Intelligence

SANS FOR578

Five-Day Program
30 CPEs
Laptop Required

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

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Validate information received from other organizations to minimize resource expenditures on bad intelligence
- Leverage open-source intelligence to complement a security team of any size
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX.

"Outstanding course material and instructor presentation! It truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."
-Thomas L., USAF

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is 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.

Cyber 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. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

"I absolutely loved this class! The instructor provided a great framework for CTI that I will use to be more effective."
-Nate DeWitt, eBay, Inc.

THERE IS NO TEACHER BUT THE ENEMY!

TRAINING EVENTS

Secure India
Bangalore | 27 Feb - 3 Mar

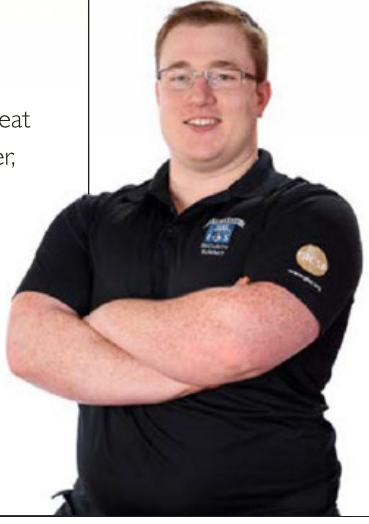
Secure Singapore
20-24 March

Cyber Defence Canberra
26-30 June

Tokyo Autumn
16-20 October

Who Should Attend

- Incident response team members
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level



SANS FOR585

Advanced Smartphone Forensics

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Secure Singapore
20-25 March

Sydney
20-25 November

www.giac.org/gasf

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

Who Should Attend

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

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. **FOR585: Advanced Smartphone Forensics** will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data are saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting the data is your job, and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

"This class exceeded my expectations. The material is cutting edge!"
-Kevin McNamara, San Diego Police Dept.

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you're working on the day you finish the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's 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!

Author Statement

Digital forensic investigations almost always involve a smartphone or mobile device. Often, the smartphone is the only form of digital evidence relating to the investigation and is the most personal device a person owns! Let's be honest: how many people share their smartphones like they do computers? Not many. Knowing how to recover all of the data residing on the smartphone is now an expectation in our field, and examiners must understand the fundamentals of smartphone handling, data recovery, accessing locked devices, and manually recovering data hiding in the background on the device. FOR585: Advanced Smartphone Forensics provides this required knowledge to beginners in mobile device forensics and to mobile device experts. This course has something to offer everyone! There is nothing out there that competes with this course. -Heather Mahalik

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS FOR610

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.

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 is a highly valuable course that equips one with the necessary skill to start on malware reverse engineering." -Kelvin Heng, DSTA

This course will teach you how to handle self-defending malware. You'll learn how 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 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.

"For those considering the cybersecurity field, this is a must."
-David First, Chevron

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Secure Singapore
13-18 March

Tokyo Autumn
16-21 October

Sydney
20-25 November

www.giac.org/grem

www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

SANS ICS410

ICS/SCADA Security Essentials

Five-Day Program
30 CPEs
Laptop Required

TRAINING EVENTS

SOS October Singapore
23-27 October

Sydney
13-17 November

www.giac.org/gicsp

www.sans.edu

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

"The material was applicable and eye opening to the possible vulnerabilities."

-Anthony Addeo, Exelon Limerick

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 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.

"Great introduction into ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company."-Mike Poulos, Coca-Cola Enterprises

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.

Managing Security Operations: Detection, Response, and Intelligence

SANS MGT517

NEW!

Five-Day Program
30 CPEs
Laptop Recommended

TRAINING EVENT

SOS October Singapore
23-27 October

Managing Security Operations entails the design, build, operation, and ongoing growth of all facets of the security capability of the organization. An effective SOC has many moving parts and must be designed with the ability to adjust and work within the constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas: Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- Business alignment and ongoing adjustment of capabilities and objectives
- Designing the SOC and the associated objectives of functional areas
- Software and hardware technology required for performance of functions
- Knowledge, Skills and Abilities of staff roles as well as hiring and cultivating staff
- Execution of ongoing operations

You will walk out of this course armed with a roadmap to design, build, and operate an effective SOC tailored to the needs of your organization.

Who Should Attend

- Information security managers
- SOC managers, analysts, and engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/system administration/ network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

Author Statement

The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for a specialist to look only at her piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a security operations center as a tool, and not the unification of people, processes, and technologies.

This course provides a comprehensive picture of what a Cyber Security Operations Center (CSOC or SOC) is. Discussion on the technology needed to run a SOC are handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. Staff roles needed are enumerated. Informing and training staff through internal training and information sharing is addressed. The interaction between functional areas and data exchanged is detailed.

After attending this class, the participant will have a roadmap for what needs to be done in the organization seeking to implement security operations.

-Chris Crowley

SANS
AUD507

Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program
36 CPEs
Laptop Required

TRAINING EVENTS

Sydney
13-18 November

www.giac.org/gsna

www.sans.edu

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

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

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? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

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 are taken from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these 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 automatically validate defenses through instrumentation and automation of audit checklists.

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

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

"The entire course has been fantastic – it far exceeded my expectations. I think SANS training is far superior to other training programs."
-Paul Petrasko, Bemis Company

SKILL-BASED SHORT COURSE

MGT433

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

Two-Day Course | 12 CPEs | Laptop NOT NEEDED

TRAINING EVENTS

Secure Canberra
13-141 March

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers, as well. Please bring example materials from your security awareness program that you can show and share with other students during the course.

Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

SANS Technology Institute
www.sans.edu

SANS Technology Institute

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

Master's Degree Programs:

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

Specialized Graduate Certificates:

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

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

GI Bill.

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

GIAC CERTIFICATIONS

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

SANS Institute offers more than 30 information security courses online via the OnDemand custom e-learning platform.

SANS OnDemand Features:

- Unparalleled faculty of information security leaders
- Four months of online access to your course
- Live subject-matter expert support
- Integrated quizzes to reinforce learning
- MP3 archives of instructor lectures
- Virtual lab access
- No travel cost
- No time away from work or home

Explore the list of courses available via OnDemand and begin studying as quickly as you like.
www.sans.org/ondemand

SPECIAL OFFERS
for OnDemand training are also available.
Learn more at sans.org/ondemand.

"Wow! This is the BEST training I have EVER encountered."

-Stanley de Jager, Symantec

It's an awesome effort: great questions, excellent material, and presentation throughout the (training event) week. I've really enjoyed it and will recommend it to many. Thank you GIAC/SANS!"
– Nicholas B., GCIH

GIAC
The Highest Standard in Cybersecurity Certification.

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

SANS | GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

WWW.GIAC.ORG

NETWARS

Information Security Challenges

Exciting and Interactive
Designed for Novice to Advanced

Play in Teams or Solo

Free for All SANS Students
Taking a 5 or 6-Day Course

"NetWars takes the concepts in the class and gives you an opportunity to put them into action."
– Kyle McDaniel, Lenovo

"Really great learning experience! Very challenging and educational!"
– Chad Eckles, Deloitte

Many ways to experience NetWars

LIVE

Core NETWARS EXPERIENCE | **DFIR NETWARS EXPERIENCE**

Free for SANS students at select SANS Training Events

ONLINE

Core NETWARS CONTINUOUS | **DFIR NETWARS CONTINUOUS**

Purchase Four Months of Online Access – New Challenges

To request a free seven day trial of Core NetWars Continuous, contact netwars@sans.org

www.sans.org/netwars

Core NetWars will be offered at:

Cyber Defence Canberra
29-30 June

Cyber Defence Japan
13-14 July

SOS October Singapore
19-20 October

DFIR NetWars will be offered at:

Secure Singapore
23-24 March

Sydney
16-17 November

SANS

The SANS Asia Pacific Team is ready to assist you

AUSTRALIA & NEW ZEALAND

Steven Armitage
sarmitage@sans.org
+61 (0)2 6287 7247
+61 402 067 768

Tory Lane
tlane@sans.org
+61 6198 3352
+61 477 005 908

INDIA

Arindam Roy
aroy@sans.org
+91 9741 900 324

INDONESIA

Mariana Tarunadjaja
mariana@sans.org
+62 815 885 6494

JAPAN

Shuji Koyanagi
skoyanagi@sans.org
+81 3 3242 6276
+81 80 6538 6030

SINGAPORE

Sean Georget
sgeorget@sans.org
+65 8612 5278
+63 908 886 5722

OTHER COUNTRIES

Ruby Souza
rsouza@sans.org
+1 808 634 0536

GENERAL INQUIRIES

AsiaPacific@sans.org
+65 6933 9540

www.facebook.com/sans.apac

twitter.com/SANSAPAC

www.linkedin.com/company/sans-apac

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 300,000 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, Phillipines, 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