The most trusted source for information security training, certification, and research.

INFORMATION SECURITY TRAINING

2018 Asia-Pacific COURSE CATALOG

80+
Certified instructors

200+
Live events globally, plus multiple online options

Curricula
Cyber Defence
Detection & Monitoring
Penetration Testing
Incident Response
Cyber Threat Intelligence

Ethical Hacking
Security Management
Audit | Legal
Secure Development
ICS/SCADA Security

“Best training I’ve attended. Great material that you can apply immediately.”
- Nik Whitis, AFG

REGISTER AT www.sans.org
CONTACT US AT AsiaPacific@sans.org
AUSTRALIA +61 2 6198 3352
JAPAN +81 3 3242 6276
SINGAPORE +65 69 339 540
Table of Contents

1 About SANS
2 SANS Training Formats
3 Build a High-Performing Security Organization
4 SANS Training Roadmap
6 SANS Event Schedule
8 Securing Approval and Budget for Training
9 SANS Baseline Skills
   Core Security Techniques
10 SEC401: Security Essentials Bootcamp Style
11 SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
12 SEC503: Intrusion Detection In-Depth
13 SEC511: Continuous Monitoring and Security Operations
14 SEC301: Intro to Information Security
15 SEC660: Enterprise Threat and Vulnerability Assessment
17 SEC545: Cloud Security Architecture and Operations
18 SEC555: SIEM with Tactical Analytics
19 SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
20 SEC579: Virtualization and Software-Defined Security
21 SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses
22 SANS NetWars Cyber Ranges
23 SANS Intermediate and Specialised Skills
   Penetration Testing & Vulnerability Analysis
24 SEC560: Network Penetration Testing and Ethical Hacking
25 SEC542: Web App Penetration Testing and Ethical Hacking
26 SEC573: Automating Information Security with Python
27 SEC575: Mobile Device Security and Ethical Hacking
28 SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
29 SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
30 SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
31 SANS Intermediate and Specialised Skills
   Incident Response and Enterprise Forensics
32 FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
33 FOR572: Advanced Network Forensics and Analysis
34 FOR500: Windows Forensic Analysis
35 FOR518: Mac Forensic Analysis
36 FOR578: Cyber Threat Intelligence
37 FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
38 SANS Security Awareness Training Products
39 SANS Intermediate and Specialised Skills
   Management | ICS Security | Software Security
40 MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™
41 MGT517: Managing Security Operations: Detection, Response, and Intelligence
42 ICS410: ICS/SCADA Security Essentials
43 ICS515: ICS Active Defense and Incident Response
44 DEV540: Secure DevOps and Cloud Application Security
45 GIAC Certification
46 SANS Asia-Pacific Team
SANS Institute’s mission is to deliver cutting-edge information security knowledge and skills to companies, military organisations, and governments in order to protect people and assets.

CUTTING-EDGE TRAINING
More than 55 unique courses are designed to align with dominant security team roles, duties, and disciplines. They prepare students to meet today’s threats and tomorrow’s challenges.

The SANS curriculum spans Cyber Defence, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Pen Testing, Industrial Control Systems Security, Secure Software Development, and more. Each curriculum offers a progression of courses that can take professionals from a subject’s foundations right up to top-flight specialisation.

We constantly update and rewrite these courses to teach the tools and techniques that are proven to keep networks safe. Our training is designed to be practical. Students are immersed in hands-on lab exercises built to let them practice, hone, and perfect what they’ve learned.

LEARN FROM EXPERTS
SANS courses are taught by an unmatched faculty of active security practitioners. Each instructor brings a wealth of real-world experience to every classroom – both live and online. SANS instructors work for high-profile organisations as red team leaders, CISOs, technical directors, and research fellows.

Along with their respected technical credentials, SANS instructors are also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom dynamic and effective.

WHY SANS IS THE BEST TRAINING AND EDUCATIONAL INVESTMENT
SANS immersion training is intensive and hands-on, and our courseware is unrivaled in the industry.

SANS instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and training content. SANS training strengthens a student’s ability to achieve a GIAC certification.

THE SANS PROMISE
At the heart of everything we do is the SANS Promise: Students will be able to deploy the new skills they’ve learned as soon as they return to work.

HOW TO REGISTER FOR SANS TRAINING
The most popular option to take SANS training is to attend a 5- or 6-day technical course taught live in a classroom at one of our 200+ training events held globally throughout the year. SANS training events provide an ideal learning environment and offer the chance to network with other security professionals as well as SANS instructors and staff.

SANS training can also be delivered online, with several convenient options to suit your learning style. All SANS online courses include at least four months of access to the course material anytime and anywhere, enabling students to revisit and rewind content.

Students can learn more and register online by visiting www.sans.org/online.
SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Training Events
Our most recommended format, live SANS training events feature SANS’s top instructors teaching multiple courses at a single time and location. This allows for:
• Focused, immersive learning without the distractions of your office environment
• Direct access to SANS Certified Instructors
• Interacting with and learning from other professionals
• Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Summits
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses
Same SANS courses, courseware, and labs are taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes
Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.

Online Training
SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certifications each year.

Top reasons to take SANS courses online:
• Learn at your own pace, over four months
• Spend extra time on complex topics
• Repeat labs to ensure proficiency with skills
• Save on travel costs
• Study at home or in your office

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

“I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time.”
- Kevin E., U.S. Army

“The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life.”
- Dan Trueman, Novae PLC
Build a High-Performing Security Organization

SANS recommends three strategies for building an information security group, based on our research and observations globally:

1 - Use practical organizing principles to design your plan and efforts. Nearly all of the more complex frameworks may be reduced to four or five simpler constructs, such as “Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents.”

2 - Prioritize your efforts within these areas using the CIS Critical Controls as you mature your own organization.

3 - Determine the number and type of professionals you require to perform the hands-on work. Engage in a persistent campaign to develop professionals with the appropriate skills and capabilities. Cybersecurity is a specialized practice area within IT and demands specialized training.

- Every professional entrusted with hands-on work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents when they occur. Set a high bar for the baseline set of skills in your security organization.

- Four job roles typically emerge as organizations grow in size and risk/complexity:
  - **Security Monitoring & Detection Professionals** – The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Vendor training all too often teaches to the tool, and not how or why the tool works, or how best it can be deployed. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and interpret their output.
  - **Pen Testers & Vulnerability Analysts** – The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking and different tools, but is essential for defense specialists to improve defenses.
  - **Forensic Investigators & Incident Responders** – Whether you’re seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.
  - **Security Managers** – With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

- Within (or beyond) these four areas, high-performing security organizations will develop individual professionals to either utilize advanced skills generally, or to meet specialized needs. Along the entire spectrum, from Active Defense to Cloud Defense to Python for Pen Testers to Malware Reverse Engineering, SANS offers more than 30 courses for specialized roles or more advanced topics, meeting the needs of nearly all security professionals at every level.

**Advanced Skills & Specialized Roles, including:**
- Blue Team Operations
- Threat Hunting
- ICS-SCADA
- Secure Development
- Active Defense
- Mobile
- Malware Reverse Engineering
- Legal & Audit

**People & Skills = f (Size of Organization, Value at Risk)**

**Value at Risk**
- Vulneration Analysis & Pen Testing
- Incident Response & Forensic Investigations
- Monitoring & Detection
- Security Managers

**Size of Organization**
- Professionals with Baseline Defensive Security Capabilities

---

VIEW THE SANS TRAINING ROADMAP to match courses to associated training paths, job roles, and skills. p.4
Baseline Skills

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

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

Core Security Techniques

Defend & Maintain

Every security professional should know the defence-in-depth techniques taught in SEC401. SEC504 completes the “offence informs defence” preparation that teaches defence specialists how attacks occur and how to respond. If you’ve got the preparation that teaches defence specialists how to respond, you should know the fundamentals of core security techniques.

Focus Job Roles

Focus Job Roles

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

Security Monitoring & Detection

SEC503 Intrusion Detection In-Depth

GCI Certification

Certified Intrusion Analyst (p. 12)

SEC511 Continuous Monitoring and Security Operations

GMON Certification

Continuous Monitoring (p. 13)

Penetration Testing & Vulnerability Analysis

SEC560 Network Penetration Testing and Ethical Hacking

GPEN Certification

Penetration Tester (p. 24)

SEC542 Web App Penetration Testing and Ethical Hacking

GWAPT Certification

Web Application Penetration Tester (p. 25)

Incident Response and Enterprise Forensics

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting

GCFA Certification

Forensic Analyst (p. 32)

FOR572 Advanced Network Forensics and Analysis

GNFA Certification

Network Forensic Analyst (p. 33)

New to Cybersecurity?

SEC301 Intro to Information Security

GIFS Certification

Information Security Professional (p. 14)

Crucial Skills, Specialised Roles

3 You are a candidate for specialised or advanced training

Cyber Defence Operations

SEC460 Enterprise Threat & Vulnerability Assessment (p. 15)
SEC501 Advanced Security Essentials – Enterprise Defender GGED (p. 15)
SEC505 Securing Windows & PowerShell Automation | GCWN
SEC506 Securing Linux/Unix | GCUX
SEC545 Cloud Security Architecture and Operations (p. 17)
SEC555 SIEM with Tactical Analytics (p. 18)
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | GCCC (p. 19)
SEC579 Virtualization and Software-Defined Security (p. 20)
SEC599 Defeating Advanced Adversaries – Implementing Kill Chain Defenses (p. 21)

Industrial Control Systems Security

ICS540 ICS/SCADA Security Essentials | GICSP (p. 42)
ICS456 Essentials for NERC Critical Infrastructure Protection
ICS515 ICS Active Defense and Incident Response | GRID (p. 43)

Penetration Testing & Ethical Hacking

SEC550 Active Defense, Offensive Countermeasures and Cyber Deception
SEC561 Immersive Hands-On Hacking Techniques
SEC573 Automating Information Security with Python GPYC (p. 26)
SEC575 Mobile Device Security and Ethical Hacking GMOB (p. 27)

Digital Forensics and Incident Response

FOR500 Windows Forensic Analysis | GCFE (p. 34)
FOR518 Mac Forensic Analysis (p. 35)
FOR526 Memory Forensics In-Depth
FOR578 Cyber Threat Intelligence | GCTI (p. 36)
FOR858 Advanced Smartphone Forensics | GASF
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GREM (p. 37)

Software Security

DEV522 Defending Web Applications Security Essentials GWEB
DEV540 Secure DevOps and Cloud Application Security (p. 44)
DEV541 Secure Coding in Java/JEE: Developing Defensible Applications | GSSP-JAVA (p. 10)
DEV544 Secure Coding in .NET: Developing Defensible Applications | GSSP-.NET

Management

MGT514 IT Security Strategic Planning, Policy, and Leadership | GSTRT
MGT517 Managing Security Operations: Detection, Response, and Intelligence (p. 41)
MGT525 IT Project Management, Effective Communication, and PMI® Exam Prep | GCPM

Audit | Legal

AUD507 Auditing & Monitoring Networks, Perimeters, and Systems | GSNR
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | GCCC (p. 19)
LEG523 Law of Data Security and Investigations | GLEG

MGT is a registered trademark of the Project Management Institute, Inc.
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Location</th>
<th>Singapore</th>
<th>Listing Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Intro to Information Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture NEW**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations NEW!</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics NEW!</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC579</td>
<td>Virtualization and Software-Defined Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Implementing Kill Chain Defenses NEW!</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC617</td>
<td>Wireless Ethical Hacking, Penetration Testing, and Defenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac Forensic Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics and Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT517</td>
<td>Managing Security Operations: Detection, Response &amp; Intelligence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS510</td>
<td>ICS/SCADA Security Essentials</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS515</td>
<td>ICS Active Defense and Incident Response</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetWars</td>
<td>Core NetWars, Cyber Defense NetWars, DFIR NetWars</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Course currently in development for release in 2018.
Write a formal request

• All organisations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.

• Provide all the necessary information in one place. In addition to your request, provide context by including information about SANS, your training path, a course description, an instructor bio and additional benefits found in this brochure or on the SANS website.

Be specific

• How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.

• Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Establish longer-term expectations

• Information security is a specialised career path within IT, with practices that evolve as attacks change. Because of this, organisations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.

• Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.

• Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
The foundation of a successful career in information security – whether technical or managerial – should be comprehensive and rooted in real-world expertise. Learn more about the SANS courses and certifications recommended for baseline skills below and on the pages that follow in this catalog.

**Core Security Techniques**

**Defend & Maintain**

<table>
<thead>
<tr>
<th>Course</th>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
</tr>
<tr>
<td>GSEC</td>
<td>Certification</td>
<td>Security Essentials</td>
</tr>
<tr>
<td>GCIIH</td>
<td>Certification</td>
<td>Certified Incident Handler</td>
</tr>
</tbody>
</table>

**Summary:** Every hands-on technical professional should possess the baseline set of knowledge and skills taught in SEC401 and SEC504. These courses cover the essentials of defence-in-depth, the mental model for how attacks work, and the proven methods for handling incidents when they occur.

**Who This Path Is For:** Hands-on technical professionals such as network administrators and engineers, security analysts, and consultants who need well-rounded and effective baseline security skills.

**Why This Training Is Important:** This training gives you essential knowledge and understanding about how a variety of attacks occur and how to respond to them.

“**The focus on methodologies was superb because the techniques taught are applicable to every environment regardless of the tools utilised.**”

- Conrad Bovell, DSS

“**This is great training that shows you potential indicators of compromise and the tools and techniques to look for and identify potentially compromised systems.**”

- Stephen Larkin, Exekib Corporation
This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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 organisations 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 organisation’s critical information assets and business systems. Our course will show you how to prevent your organisation’s security problems from being headline news in the Wall Street Journal!

Prevention Is Ideal but Detection Is a Must.

With the rise in advanced persistent threats, it is almost inevitable that organisations will be targeted. Whether the attacker is successful in penetrating an organisation’s network depends on the effectiveness of the organisation’s defence. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organisations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defence. Before your organisation 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 defence. 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 organisations. 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 course has been the best training I have ever taken from an instructor with the knowledge and ability to teach the material.”

- J. O. Lordi, Wawa
The Internet is full of powerful hacking tools and bad guys using them extensively. If your organisation has an Internet connection and 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.

“This course really provides great insights on how to protect our infrastructures.”

-SANJEEV SINGH, INDIAN NAVY

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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. This course will enable you to discover the holes in your system before the bad guys do!

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

“[This course is a] good foundation for security incidents. It’s a must-have for security incident handlers/managers.”

-WU PEIHUI, CITIBANK
Reports of prominent organisations 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. 

“This course met my expectations, providing clear and concise information from an instructor who did an excellent job keeping the material and course interesting – well done.” -DAVID HOLLAND, STROZ FRIEDBERG

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 emphasises 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.

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.

---

“IT is easy to relate the course material directly to real-world scenarios and understand how I will apply the skills at work.”

- JARED ANTHONY,
SECURITY RISK ADVISORS

“This course directly covers the necessary knowledge and skill set I use day to day for my job. The added insight is worth the price of the course.”

- MICHAEL GARRETT,
FEDERAL RESERVE BANK OF SAN FRANCISCO
SEC511
Continuous Monitoring and Security Operations

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

Training Events
- Secure Singapore 12-24 Mar
- Melbourne 21-26 May
- Philippines Manila | 18-23 June
- Tokyo Autumn 3-15 Sep
- October Singapore 15-27 Oct
- Bangalore 3-8 Dec

We continue to underestimate the tenacity of our adversaries! Organisations are investing significant time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organisations 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 organisations to detect threats that will inevitably slip through their defences.

The underlying challenge for organisations victimised 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 organisations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organisation or Security Operations Center (SOC) to analyse threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will 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 utilising 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!
To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

➢ Do you have basic computer knowledge, but are 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 (with some technical knowledge) 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 a basic knowledge of computers and technology but no prior knowledge of cybersecurity. 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.

“Labs reinforced the security principles in a real-world scenario.”
- TYLER MOORE, ROCKWELL

“This course presents a unique opportunity to learn the broad scope of information security with a knowledgeable instructor and superior training material.”
- IRA HUBERT, FEDEX
Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organisations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from organisations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools, and a proven testing methodology.

This course takes you beyond the checklist, giving you a tour of the attackers’ perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasises this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyse and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your medium- or large-scale organisation.
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 appropriately respond 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.

“The hands-on lab approach is a great way to make sense of what is being taught, and working with other classmates helped expand our knowledge and brought cohesion.”

- RACHEL WEISS, UPS INC.

Of course, despite an organisation’s best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organisations 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 organisation 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 preventive and detective measures, completing the security lifecycle.

Author Statement

“I started off working as a network engineer and architect building enterprise networks. This role organically transitioned into secure design and engineering. My interest at the time in penetration testing and exploitation allowed me to verify that our designs being put into production were truly hardened. This interest eventually drove me into a career in full-blown reverse engineering and 0-day bug discovery/exploit development. After a long history of writing and teaching courses for SANS on advanced penetration testing and exploit writing, I am excited to take that experience and apply it back into defense. We selected a group of rock star authors to build the SEC501 syllabus and content, including Dave Shackleford, Phil Hagen, Matt Bromiley, and Rob Davenport.”

- Stephen Sims
As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But, will information security prove to be an Achilles’ heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

The SEC545 course, Cloud Security Architecture and Operations, will tackle these issues one by one. We’ll start with a brief introduction to cloud security fundamentals, and then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we’ll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We’ll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We’ll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We’ll devote an entire day to adapting our offense and defense focal areas to cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we’ll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration and every facet of the cloud life cycle. We’ll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.
## SEC555

### SIEM with Tactical Analytics  NEW!

<table>
<thead>
<tr>
<th>Six-Day Program</th>
<th>46 CPEs</th>
</tr>
</thead>
</table>

**Who Should Attend**

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

**Training Events**

- **Secure Singapore**  
  12-24 Mar
- **Cyber Defence Canberra**  
  25 June - 7 July
- **Tokyo Autumn**  
  3-15 Sep
- **Bangalore**  
  3-8 Dec

Many organisations have logging capabilities but lack the people and processes to analyse it. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide individuals with training, methods, and processes for enhancing existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilises SOF-ELK, a free, SANS-sponsored Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a “big data” problem but rather a “data analysis” problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This course moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the “appropriate” use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyse key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions.

Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilising modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualisations.
Implementing and Auditing the Critical Security Controls – In-Depth

Who Should Attend

> Information assurance auditors
> System implementers or administrators
> Network security engineers
> IT administrators
> Department of Defence personnel or contractors
> Staff and clients of federal agencies
> Private sector organisations 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

Training Events

> October Singapore
  15–27 Oct

“Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organisation 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 organisation’s security should too. To enable your organisation 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 prioritised, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defences. They are designed to complement existing standards, frameworks, and compliance schemes by prioritising the most critical threats and highest payoff defences, 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.”

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.
Virtualization and Software-Defined Security

Five-Day Program
30 CPEs
Laptop Required

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

Training Events
> Secure Singapore
12-24 Mar

One of today’s most rapidly evolving and widely deployed technologies is server virtualisation. SEC579: Virtualization and Software-Defined Security is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures, as well as understand software-defined networking and infrastructure security risks.

Many organisations are already realising cost savings from implementing virtualised servers, and systems administrators love the ease of deployment and management of virtualised systems. More and more organisations are deploying desktop, application, and network virtualisation as well. There are even security benefits of virtualisation: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

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

In addition, many organisations are evolving virtualised infrastructure into private clouds using converged infrastructure that employs software-defined tools and programmable stack layers to control large, complex data centers. Security architecture, policies, and processes will need to be adapted to work within a converged infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure that assets are protected.

This course will cover core operational functions such as secure network design and segmentation, building secure systems, and secure virtualisation implementation and controls. Cutting-edge topics like software-defined networking and container technology will also be covered in detail with an emphasis on security techniques and controls. Security-focused virtualisation, integration, and monitoring will be covered at length. Attacks and threats to virtual environments will be discussed, and students will learn how to perform vulnerability assessments and penetration tests in their virtual environments. We’ll also look at how to implement network intrusion detection and access controls, implement log and event management, and perform forensics and incident handling in virtual and converged data centers. Finally, students will learn how to perform technical audits and assessments of their in-house and public cloud environments, creating reports and documenting technical controls. This instruction will heavily emphasise automation and scripting techniques.

“SEC579 was one of the best-produced SANS courses I have taken. The blend of ops and security was extremely valuable.”
-SCOTT TOWERY, VISIONS

“Great course! Anyone involved with managing virtual system environments will benefit.”
-RANDALL RILEY, DEFENSE SECURITY SERVICES
You just got hired to help our virtual organisation “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: “We really don’t know where to start! We looked at some recent cybersecurity trend reports and we feel like we’ve lost the plot. Advanced persistent threats, ransomware, denial of service—we’re not even sure where to start!”

Cyber threats are on the rise: ransomware is affecting small, medium and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels.

SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses will arm you with the knowledge and expertise you need to detect and respond to today’s threats. Recognising that a prevent-only strategy is not sufficient, we will introduce security controls designed to stop advanced adversaries.

Course authors Erik Van Buggenhout and Stephen Sims (both certified as GIAC Security Experts) are hands-on practitioners who have achieved a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked “But how do I prevent this type of attack?” With more than 20 labs plus a full-day “Defend-The-Flag” exercise during which students attempt to defend our virtual organisation from different waves of attacks against its environment, SEC599 gives students real world examples of how to prevent attacks.

Our six-day journey will start with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce the Advanced Persistent Threat (APT) Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organisation “SyncTechLabs” in our Day 1 exercises.

Throughout days two through five, we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. In designing the course and its exercises, the authors went the extra mile to ensure that attendees “build” something that can be used later on. For this reason, the different technologies illustrated throughout the course (e.g., IDS systems, web proxies, sandboxes, visualisation dashboards, etc.) will be provided as usable virtual machines on the course USB.

SEC599 will finish with a bang. During the “Defend-the-Flag” challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?
The all-new NetWars Defence Competition is a defence-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. With so much focus on offence, NetWars Defence is a truly unique experience and opportunity to test your skills in architecture, operations, threat hunting, log analysis, packet analysis, cryptography, and much more!

Who Should Attend

- System administrators
- Enterprise defenders
- Architects
- Network engineers
- Security operations specialists
- Incident responders
- Security analysts
- Security auditors
- Builders and breakers

The Core NetWars Experience is a computer and network security challenge designed to test participants’ experience and skills in a safe, controlled environment while having a little fun with their fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you’ll build a wide variety of skills while having a great time.

Who Should Attend

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

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

Who Should Attend

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

Introducing: Experience 5.0

“A Whole New Experience!”
Summary: High-performing security organisations need specially trained professionals who can continuously challenge the defences and monitoring systems set up by the cyber defence operations teams, and discover vulnerabilities to be addressed that might otherwise be exploited by attackers. Professionals focusing on this career path must be able to test both network and wireless vulnerabilities and understand these environments before advancing to additional areas.

SEC560 and SEC542 teach you the skills that are core to this type of role. An additional nine SANS penetration testing courses in advanced and specialised topics allow you to mold your career into a particular practice area or task. Review the following pages for detailed information about all of these courses and the certifications that validate your acquired skills.

Who This Path Is for: Information security engineers, analysts, and risk consultants need to master this coursework to hone their penetration testing, ethical hacker, and vulnerability analysis skills.

Why This Training Is Important: These courses teach proper planning, scoping, and recon, and dive deep into scanning, target exploitation, password attacks, web app configuration, identity and authentication, custom scripting, and interception proxies. This training, which includes dozens of detailed, hands-on labs, allows you to go back to work with the practical, real-world examples and practice needed to do your job efficiently and masterfully.

“I was pleasantly humbled, challenged, encouraged and trained. I feel 100% more qualified to defend my company’s network after taking this training.”

-Ivan Dominguez, NWCU.com
Network Penetration Testing and Ethical Hacking

As a cybersecurity professional, you have a unique responsibility to find and understand your organisation’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 organisation 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 more than 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.

“I learned more in one class than in years of self-study!”

- BRADLEY MILHORN, COMPUCOM INC.

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 organisation, demonstrating the knowledge you’ve mastered in this course.

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

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 emphasise the importance of defence in depth.
Web applications play a vital role in every modern organisation. However, if your organisation doesn’t properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organisations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, 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 organisation. Unfortunately, there is no “patch Tuesday” for custom web applications, and 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 defence 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 organisations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organisations. Even technically gifted security geeks often struggle with helping organisations 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 organisation to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organisations through penetration testing, and not just show off hacking skills. This 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 having 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 that hammers home lessons learned.
Automating Information Security with Python

SEC573

Six-Day Program
36 CPEs

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

Training Events

➢ Secure Singapore
  12-24 Mar
➢ August Sydney
  20-25 Aug

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.

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.

Finally, what do you do when “off-the-shelf” tools and exploits fall short? As a penetration tester you need to evolve as quickly as the threats you are paid to emulate, so the answer is simple, if you have the skills: 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 in 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.

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

“SEC573 gave me exposure to tools and techniques I wouldn’t have normally considered, but now are part of my arsenal.”
-Allen C., Department of Defense
Imagine an attack surface spread throughout your organisation 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 organisations, yet these same organisations 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 characterise 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 organisations 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.
SEC617

Wireless Ethical Hacking, Penetration Testing, and Defenses

Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, it is growing in deployment and utilisation with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies like ZigBee and Z-Wave offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, Bluetooth Low Energy, and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

"Valuable training that I will recommend to my colleagues."
-ERIC T., CANADIAN GOVERNMENT

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you’ll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you’ll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. You’ll also develop attack techniques leveraging Windows 7 and Mac OS X. We’ll examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you’ll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

You Will Be Able To

- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, CarWhisperer, and btaptap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- Utilise wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organisation
- Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilise wireless fuzzing tools including Metasploit file2air, and Scapy to identify new vulnerabilities in wireless devices

WHO SHOULD ATTEND

- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

TRAINING EVENTS

- Cyber Defence Canberra
  25 June – 7 July
- October Singapore
  15-27 Oct

“SEC617 is great for someone looking for a top to bottom rundown in wireless attacks.”
-GARET PICCHIONI, SALESFORCE

“Clear and clean presentation of wireless security. Easy to understand with real-life stories to back them up.”
-ERICH WINKLER, COSTCO WHOLESALE

GAWN Certification
Assessing and Auditing Wireless Networks
www.giac.org/gawn

With this course

www.sans.org/ondemand
Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Six-Day Program
36 CPEs

Who Should Attend
- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

Training Events
- Secure Japan
  Tokyo   |   19 Feb - 3 Mar
- Melbourne
  21-26 May

“SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills.”
-MATTHEW SULLIVAN, WEBFILINGS

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?
Modern web applications are growing more sophisticated and complex as they utilise exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?
This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills
We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We’ll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We’ll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

Author Statement
“As web applications and their mobile counterparts become more complex and hardened against attack, penetration testers need to continually update the techniques and tools they use to evaluate the security of these systems. This includes understanding how the various new technologies work, which tools work with cutting-edge technologies like HTTP2 and NoSQL, how to perform special penetration tests like Web Application Firewall inspections, and how to perform custom exploitation to demonstrate maximum impact for the applications you test. This course is designed to expand past the methodology and the ‘how’ when we are presented with the challenges of web penetration testing, and dig into the more esoteric ‘why’ these techniques and tools work, so that you can adapt as needed in your assessments.”

Justin Searle

Course Author
Justin Searle

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/courses
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SEC660

Six-Day Program
46 CPEs

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

Training Events
- Secure Singapore
  12-24 Mar
- Cyber Defence Japan
  Tokyo  |  18-30 June
- Cyber Defence Canberra
  25 June - 7 July
- October Singapore
  15-27 Oct
- Sydney
  5-17 Nov

“...the SEC660 course was hands-on, packed with content, and current to today’s technology!”
- Michael Horken, Rockwell Automation

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 weaponising 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.

GXPN Certification
Exploit Researcher and Advanced Penetration Tester

www.giac.org/gxpn

www.sans.org/ondemand

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

“...the SEC660 course was hands-on, packed with content, and current to today’s technology!”
- Michael Horken, Rockwell Automation

www.sans.org/ondemand
SANS Intermediate and Specialised Skills
Incident Response and Enterprise Forensics

Summary: Properly trained incident responders can hunt for and identify compromised systems, provide effective containment during a breach, and rapidly remediate an incident. They must have in-depth digital forensics knowledge of both host and network systems within the enterprise and know how to apply proactive threat intelligence – skills taught by SANS in FOR508, FOR572, and FOR578.

Specialised incident response and forensics skills are taught in six additional SANS courses, covering everything from Windows forensics to reverse engineering malware. Review the following pages for detailed information about all of these courses.

Who This Path Is for: Incident responders, cyber threat analysts, forensic examiners, security analysts and engineers all utilise this training path to advance their threat hunting and responding skills.

Why This Training Is Important: This training will teach you to detect compromised and affected systems, how and when a breach occurred, what attackers took or changed, and how to contain and remediate incidents. Upon completing your focus path in incident response and enterprise forensics, you will be able to incorporate evidence from different sources such as networks, mobile devices, and more into your investigations, provide better findings, and get the job done faster.

“This training gave me immediately applicable skills from active professionals in the field.”
-Abe Jones, Spectrum Health
Advanced Digital Forensics, Incident Response, and Threat Hunting

Six-Day Program
36 CPEs

Who Should Attend
> Incident response team members
> Threat hunters
> Experienced digital forensic analysts
> Information security professionals
> Federal agents and law enforcement
> Red team members, penetration testers, and exploit developers
> SANS FOR500 and SEC504 graduates

Training Events
> Secure Japan
  Tokyo   |   19 Feb - 3 Mar
> Secure India
  Bangalore   |   12-17 Feb
> Secure Canberra
  19-24 Mar
> Melbourne
  21-26 May
> Cyber Defence Singapore
  9-14 July
> August Sydney
  20-25 Aug
> Tokyo Autumn
  3-15 Sep
> October Singapore
  15-27 Oct
> Osaka
  12-17 Nov

FOR508: Advanced Digital Forensics, Incident Response, and Threat 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 organisations like yours, and that your organisation 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 organisation’s networks. Organisations 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 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, organised 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.

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

“This is, by far, the best training I have ever had. My forensic knowledge increased more in the last week than in the last year.”
-Vito Rocco, UNLV
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/courses

Training Events

- **Cyber Defence Japan**
  - Tokyo | 18-30 June

- **Cyber Defence Canberra**
  - 25 June - 7 July

- **October Singapore**
  - 15-27 Oct

"Immediately applicable skills from an active professional in the field."

- **Abe Jones, Spectrum Health**

"Great training course that is exposing me to new networking concepts."

- **John McDonald, Florida Dept. of Law Enforcement**

**FOR572: Advanced Network Forensics and Analysis**

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn’t have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

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

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way. Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters,” this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC 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 FOR500 (formerly 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 the use of disk or memory images.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfdump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform – a VMware appliance pre-configured with the ELK stack. This “big data” platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.
Six-Day Program
36 CPEs

Who Should Attend
- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR500 (formerly FOR408) and SEC504 graduates

Training Events
- Secure Japan
  Tokyo | 19 Feb - 3 Mar
- Secure Singapore
  12-24 Mar
- Cyber Defence Canberra
  25 June - 7 July
- Sydney
  5-17 Nov

“IT’s the best Windows forensic class in the world.”
- Bob A. Akin, SALC

“This is the best course I have taken in 20 years.”
- Mauricio Bellido Jr, USG

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

All organisations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital 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 experts capable of piecing together what happened on computer systems second by second.

“This is a great look at forensic tools, acquiring data, and how they pertain to real-world scenarios.” – Rick Schroeder, Penn Medicine

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can’t protect what you don’t know about, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn how to recover, analyse, and authenticate forensic data on Windows systems, track particular user activity on your network, and organise 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 unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques, prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyse everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500: Windows Forensic Analysis will teach you to:
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

www.sans.org/ondemand

“IT’s the best Windows forensic class in the world.”
- Bob A. Akin, SALC

“This is the best course I have taken in 20 years.”
- Mauricio Bellido Jr, USG

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can’t protect what you don’t know about, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn how to recover, analyse, and authenticate forensic data on Windows systems, track particular user activity on your network, and organise 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 unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques, prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyse everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500: Windows Forensic Analysis will teach you to:
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

www.sans.org/ondemand

“IT’s the best Windows forensic class in the world.”
- Bob A. Akin, SALC

“This is the best course I have taken in 20 years.”
- Mauricio Bellido Jr, USG

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can’t protect what you don’t know about, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn how to recover, analyse, and authenticate forensic data on Windows systems, track particular user activity on your network, and organise 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 unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques, prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyse everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500: Windows Forensic Analysis will teach you to:
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

www.sans.org/ondemand

“IT’s the best Windows forensic class in the world.”
- Bob A. Akin, SALC

“This is the best course I have taken in 20 years.”
- Mauricio Bellido Jr, USG
FOR 518

Mac Forensic Analysis

Six-Day Program
36 CPEs

Who Should Attend

› Incident response team members
› Threat hunters
› Experienced digital forensic analysts
› Security Operations Center personnel and information security practitioners
› Federal agents and law enforcement officials
› SANS FOR500, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

Training Events

› Sydney
5-17 Nov

“Best of any course I’ve ever taken. I love the idea of being able to bring the material home to review.”

- Eric Koebelen,
Incident Response US

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

“This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession.”

- Naveel Koya, AC-DAC – Trivandrum

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

FOR518: Mac Forensic Analysis will teach you:

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

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

FORENSICATE DIFFERENTLY!

Author Statement

“This course is designed to enable an analyst comfortable in Windows-based forensics to perform just as well on the Mac. The Mac market share is an ever-increasing and popular platform for many companies and government entities.

I believe a well-rounded forensic analyst is an extremely well-prepared and employable individual in a Windows forensics world. Windows analysis is the base education in the competitive field of digital forensics. Any additional skills you can acquire can set you apart from the crowd, whether it is Mac, mobile, memory, or malware analysis.

Mac forensics is truly a passion of mine that I genuinely want to share with the forensics community. While you may not work on a Mac investigation every day, the tools and techniques you learn in this course will help you with other investigations including Windows, Linux, and mobile.”

- Sarah Edwards

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/courses
FOR578: Cyber Threat Intelligence

Five-Day Program
30 CPEs

Who Should Attend
- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR500, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

Training Events
- Secure Singapore
  12-24 Mar
- Cyber Defence Japan
  Tokyo | 18-30 June
- Sydney
  5-17 Nov

Make no mistake: current network defence, 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 organisations.

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 organisations to minimise 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.

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 organisations 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 organisation 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 organisations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

Author Statement
“Before threat intelligence was a buzzword, it was something we all used to just do as part of incident response. But I’ll admit that most of us used to do it badly. Or more accurately, ad hoc at best. We simply lacked structured models for intrusion analysis, campaign tracking, and consistent reporting of threats. Today, we need analysts trained in intelligence analysis techniques ready to perform proper campaign modeling, attribution, and threat analysis. The Cyber Threat Intelligence course teaches students all of that, as well as how to avoid cognitive biases in reporting and how to use alternative competing hypothesis in intelligence analysis. These are critical skills that most in industry today absolutely lack.”
- Jake Williams
Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organisation’s ability to derive threat intelligence, respond to information security incidents, and fortify defences. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analysing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen’s capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialised tools, and how to rebuild the files’ structure to bypass the packer’s protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognise and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systemic manner. 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.

“No other malware course I have taken comes close to this course.”
-Andy Honey, NCA

“This material is something you can use to build or enhance your company’s playbook in terms of incident response and detection.”
-Chris Bailey, California Lottery
SANS Security Awareness offers computer-based training modules that enable both compliance and behavior change across a wide range of critical security topics. Over 100 different expert-authored training modules can be used across healthcare, software development, employee security awareness and industrial control systems. Phishing training is seamlessly integrated with the security awareness training program to ensure you're not just checking the box but also moving toward more secure behaviors.

Module quiz questions test learner comprehension and detailed reports allow you to track user completion and violations for compliance reporting purposes. Over 20 language options offer consistent training across your entire organization regardless of geography.
Summary: Professional security managers need broad and proven knowledge of policy, standards and practices in order to provide the greatest level of security to their organisations. They also need to speak their technicians’ language and design security plans that withstand attack from all angles. SANS’ specialised management and audit courses deliver the tools and techniques required to lead with confidence.

Who This Path Is for: CISOs, IT directors, or others with responsibility for managing their organisation’s security operations benefit from the experience-rich instruction in SANS management courses. Security, system, and network administrators who are pursuing a new management role should also prepare themselves by taking this type of training.

Why This Training Is Important: Professionals who train and certify in these skills are the leaders of cybersecurity. They master the specific techniques and tools needed to communicate information security best practices to executives and technical teams, audit the Critical Security Controls, and will design the Security Operation Centers of the future.
This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it’s like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

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

Knowledge Compression™

Maximise your learning potential!

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

“This course is highly useful for giving me a sound baseline of technical and general skills to help me manage an effective team.”
-Richard Ward, REA Group

“This was a great course that I feel all management should take. It helps managers understand not only security but also technical and business concepts and issues.”
-David Stewart, ADM

“MGT512 is one of the most valuable courses I’ve taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!”
-John Madick, EPIQ Systems, Inc.
Managing Security Operations: Detection, Response, and Intelligence

Managing security operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organisation. An effective Security Operations Center (SOC) has many moving parts and must be designed so that it can be adjusted to work within the context and constraints of the organisation. 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 of 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 as well as staff hiring and training
- Execution of ongoing operations

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

“SANS coursework is the most thorough learning available, anywhere. What you learn is not only conceptual, but also hands-on, showing you what to do, why you do it, and how you can apply solutions that you learn to real-world problems.”

-DUANE TUCKER, BARMARK PARTNERS

Author Statement

“The inclusion of all functional areas of security operations in this course is intended to develop a standardised program for an organisation 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 enterprise prevent loss due to poor security practices. I have encountered detrimental compartmentalisation in most organisations. There is a tendency for specialists to look only at their piece of the problem, without understanding the larger scope of information security within an organisation. Organisations are likely to perceive a Security Operations Center (SOC) as a tool, and not the unification of people, processes, and technologies.

“This course provides a comprehensive picture of what a Cybersecurity Operations Center is. Discussions on the technology needed to run a SOC are handled in a vendor-agnostic way. The course examines technology in a way that addresses both minimal budgets and budgets with a global scope, outlines staff roles, looks at ways to inform and train staff through internal training programs and information-sharing, and details the interaction between functional areas and data exchange.

“After attending this course, participants will have a roadmap that outlines what an organisation needs to do to implement security operations.”

-Christopher Crowley
ICS/SCADA Security Essentials

SANS has joined forces with industry leaders to equip cybersecurity 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 standardised 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 defence architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources

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

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defences 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.

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

### Training Events
- **Secure Japan**
  - Tokyo | 19 Feb - 3 Mar
- **Hyderabad**
  - 6-11 Aug
- **October Singapore**
  - 15-27 Oct

---

**“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
ICS Active Defense and Incident Response

Five-Day Program
30 CPEs

Who Should Attend

› ICS incident response team leads and members
› ICS and operations technology security personnel
› IT security professionals
› Security Operations Center (SOC) team leads and analysts
› ICS red team and penetration testers
› Active defenders

Training Events

› Tokyo Autumn
  3-15 Sep
› Wellington
  24-29 Sep

ICS515: ICS Active Defense and Incident Response will help you deconstruct cyber attacks on industrial control systems (ICS), leverage an active defence to identify and counter threats, and use incident response procedures to maintain the safety and reliability of operations.

This course will empower students to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defence. An active defence is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defence concepts such as using threat intelligence, performing network security monitoring, and utilising malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organisations looking to show that defence is do-able.

This course will prepare you to:

› Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
› Use active defence concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
› Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
› Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others
› Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELISA, Volatility, Redline, FTK Imager, PDF analysers, malware sandboxes, and more
› Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
› Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

Author Statement

“This class was developed from my experiences in the U.S. intelligence community and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you’ll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defence is do-able.”

-Robert M. Lee
This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

The first two days of the course cover how Secure DevOps can be implemented using lessons from successful DevOps security programs. Students build a secure DevOps CI/CD toolchain and understand how code is automatically built, tested, and deployed using popular open source tools such as git, Puppet, Jenkins, and Docker. In a series of labs you learn to inject security into your CI/CD toolchain using various security tools, patterns, and techniques.

The final three days of the course cover how developers and security professionals can utilize AWS services to build secure software in the cloud. Students leverage the CI/CD toolchain to push application code directly to the cloud instead of to local servers on their class virtual machines. Students analyze and fix applications hosted in the cloud using AWS services and features such as API Gateway, IAM, signed cookies, Security Token Service, autoscaling, KMS, encryption, WAF, and Lambda for Serverless computing.

The course makes extensive use of open source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring.

This course also makes extensive use of Amazon Web Services (AWS) and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

This course will prepare you to:

- Understand the core principles and patterns behind DevOps.
- Map out and implement a Continuous Delivery/Deployment pipeline
- Map out where security controls and checks can be added in Continuous Delivery and Continuous Deployment
- Integrate security into production operations
- Create a plan for introducing - or improving - security in a DevOps environment.
- Move your DevOps workflows to the cloud
- Consume cloud services to secure cloud applications
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.

“I think the exam was both fair and practical. These are the kind of real-world problems I expect to see in the field.”

– Carl Hallberg, Wells Fargo, GIAC Reverse Engineering Malware (GREM)
The SANS Asia-Pacific Team is ready to assist you

AUSTRALIA & NEW ZEALAND

Steven Armitage
sarmitage@sans.org
+61 2 6198 3352  +61 402 067 768

Tory Lane
tlane@sans.org
+61 2 6198 3352  +61 477 005 908

JAPAN

Yoshihiro Sekitori
ysekitori@sans.org
+81 90 6487 8001

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

INDIA

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

INDONESIA

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

SINGAPORE & HONG KONG

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

OTHER COUNTRIES

Ruby Souza
rsouza@sans.org
+1 904 325 1996

GENERAL INQUIRIES

AsiaPacific@sans.org

AUSTRALIA  +61 2 6198 3352  JAPAN  +81 3 3242 6276  SINGAPORE  +65 6933 9540

www.facebook.com/sans.apac  twitter.com/SANSAPAC  www.linkedin.com/company/sans-apac