INFORMATION SECURITY TRAINING

2019 Asia-Pacific COURSE CATALOG

90+ Certified instructors

200+ Live events globally, plus multiple online options

Curricula
Cyber Defence
Detection & Monitoring
Penetration Testing
Incident Response
Digital Forensics

Cyber Threat Intelligence
Ethical Hacking
Security Management
Maximising SIEMs
ICS/SCADA Security

“The courses at SANS are ALWAYS valuable immediately upon returning to work.”
- William Stott, Raytheon

The most trusted source for information security training, certification, and research.
# Table of Contents

1. About SANS
2. SANS Training Formats
3. Build a High-Performing Security Organisation
4. SANS Training Roadmap
5. SANS Event Schedule
6. SANS Faculty
7. SEC
   - SEC401 Security Essentials Bootcamp Style
   - SEC503 Intrusion Detection In-Depth
   - SEC511 Continuous Monitoring and Security Operations
   - SEC301 Introduction to Cyber Security
   - SEC487 Open-Source Intelligence (OSINT) Gathering and Analysis **NEW!**
   - SEC501 Advanced Security Essentials – Enterprise Defender **NEW!**
   - SEC530 Defensible Security Architecture **NEW!**
   - SEC545 Cloud Security Architecture and Operations
   - SEC555 SIEM with Tactical Analytics
   - SEC542 Defeating Advanced Adversaries – Implementing Kill Chain Defenses
   - SEC560 Network Penetration Testing and Ethical Hacking
   - SEC542 Web App Penetration Testing and Ethical Hacking
   - SEC460 Enterprise Threat and Vulnerability Assessment **NEW!**
   - SEC573 Automating Information Security with Python
   - SEC575 Mobile Device Security and Ethical Hacking
   - SEC517 Wireless Penetration Testing and Ethical Hacking **NEW!**
   - SEC642 Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
   - SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
   - SEC760 Advanced Exploit Development for Penetration Testers
   - FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting
   - FOR572 Advanced Network Forensics and Analysis
   - FOR500 Windows Forensic Analysis
   - FOR578 Cyber Threat Intelligence
   - FOR585 Advanced Smartphone Forensics
   - FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
   - MGT512 Security Leadership Essentials for Managers **NEW!**
   - MGT510 Security Strategic Planning, Policy, and Leadership
   - ICS410 ICS/SCADA Security Essentials
   - ICS515 ICS Active Defense and Incident Response
   - DEV540 Secure DevOps and Cloud Application Security
   - NetWars Experience
8. SANS Flagship Programs and Free Resources
At the SANS Institute, our mission is to deliver the cutting-edge information security knowledge and skills that companies, military organisations, and governments need to protect their people and assets.

**TRAINING ON THE CUTTING EDGE**

We offer more than 65 unique courses, all designed to align with dominant security team roles, duties, and disciplines. Our courses prepare students to face today’s threats and tomorrow’s challenges.

The SANS curriculum spans the full range of cybersecurity fields including Cyber Defence, Penetration Testing & Ethical Hacking, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Critical Infrastructure and Control Systems Security, Secure Software Development, and more.

In SANS courses, students are immersed in hands-on lab exercises designed to help them practice, hone, and perfect what they’ve learned. And we constantly update and rewrite our courses to be sure the tools and techniques we’re teaching are always current, and on the cutting edge.

**LEARN FROM THE BEST**

The SANS faculty is simply unmatched. All of our instructors are active security practitioners, bringing their extensive knowledge and real-world experiences directly to the classroom.

SANS instructors work for high-profile organisations as red team leaders, CISOs, technical directors, and research fellows. In addition to their respected technical credentials, they’re also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom—both live and online—dynamic and effective.

**GIAC SKILLS VALIDATION**

GIAC certifications are designed to ensure that students can apply their knowledge and skills in a real-world setting. More than 30 certifications align with SANS training courses, validating student mastery for professional use in critical, specialised InfoSec domains and job-specific roles. See [www.giac.org](http://www.giac.org) for more information.

**A TRAINING FORMAT FOR EVERY STUDENT**

SANS holds more than 300 live training events around the world each year, so you can find a convenient time and place to take your course. These events provide an engaging learning environment and multiple opportunities to network with other security professionals, SANS instructors, and staff.

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

**RECOGNISED AS A SUPERIOR INVESTMENT**

Information security professionals from every member of the Fortune 100, and from small and mid-sized firms alike, say they return to SANS training again and again because they trust their training will result in practical and high-quality capabilities. SANS training is also embedded in government and military programs in the United States and allies around the world for the same reason.

Customer feedback drives our continuous effort to maintain the quality and impact of SANS training, so that we continue to deserve your trust.

**THE SANS PROMISE**

At the heart of everything we do is the SANS Promise: Students will be able to use their new skills as soon as they return to work.

**REGISTER FOR SANS TRAINING**

Learn more about SANS courses, and register online, at [www.sans.org](http://www.sans.org)
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
SANS recommends three strategies for building an information security group, based on our research and observations globally:

1 - Use practical organising 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 Defences – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents.”

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

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 specialised practice area within IT and demands specialised training.

- Every professional entrusted with hands-on work should be trained to possess a common set of capabilities enabling them to secure systems, practice defence-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 organisation.

- Four job roles typically emerge as organisations 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 defences. 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 defence specialists to improve defences.
  - 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 organisations need specialised professionals who can move beyond first-response incident handling in order to analyse an attack and develop an appropriate remediation and recovery plan.
  - Security Managers – With an increasing number of talented technologists, organisations 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 organisations will develop individual professionals to either utilise advanced skills generally, or to meet specialised needs. Along the entire spectrum, from Active Defence to Cloud Defence to Python for Pen Testers to Malware Reverse Engineering, SANS offers more than 30 courses for specialised roles or more advanced topics, meeting the needs of nearly all security professionals at every level.

VIEW THE SANS TRAINING ROADMAP to match courses to associated training paths, job roles, and skills. p. 4
Training Roadmap | Development Paths

Baseline Skills

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

Core Techniques

Every Security Professional Should Know

Security Essentials

SEC401 Security Essentials Bootcamp Style | GSEC

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

Hacker Techniques

SEC404 Hacker Tools, Techniques, Exploits, and Incident Handling | GCIH

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

Focus Job Roles

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

Monitoring & Detection

Introsion Detection, Monitoring Over Time

Scan Packets & Networks

Introsion Detection

SECS9 Intrusion Detection In-Depth | GIAC

Monitoring & Operations

SECS9 Continuous Monitoring and Security Operations | GACO

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing

Vulnerability Analysis, Ethical Hacking

Networks

SECS90 Network Penetration Testing and Ethical Hacking | GPEN

Web Apps

SECS92 Web App Penetration Testing and Ethical Hacking | GWRAPT

The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenant 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 their defenses.

Incident Response & Threat Hunting

Host & Network Forensics

Every Forensics & IR Professional Should Know

Endpoint Forensics

FOR500 Windows Forensic Analysis | GCFE

FOR503 Advanced Digital Forensics, Incident Response, and Threat Hunting | GCSA

Network Forensics

FOR502 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GAFD

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 Management

Managing Technical Security Operations

Every Security Manager Should Know

Leadership Essentials

MG7512 Security Leadership Essentials For Managers | GSEC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. These 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.

Critical Controls

SECSX66 Implementing and Auditing the Critical Security Controls – In-Depth | GCCE

CISPP® Training

MG7416 SANS Training/Program for CISSP® Certification | GSEP

www.sans.org/courses

To learn more about additional SANS courses and the digital version of this book, visit www.sans.org/courses.
Crucial Skills, Specialized Roles

SANS’s comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

You are a candidate for specialized or advanced training

### Cyber Defense Operations

**Specialized Defensive Area**

- **Advanced Generalist**
  - SECS47: Advanced Security Essentials – Enterprise Defender | GCED
- **Cloud Security**
  - SECS48: Cloud Security Architecture and Operations
- **Windows/PowerShell**
  - SECS58: Securing Windows and PowerShell Automation | GCWN
- **Linux/Unix Defense**
  - SECS67: Securing Linux/Unix | GCUX
- **Virtualized Data Centers**
  - SECS79: Virtualization and Software-Defined Security
- **ISEM**
  - SECS01: ISEM with Tactical Analytics | GCDA
- **Other Advanced Defense Courses**
  - **Security Architecture**
    - SECS30: Defensible Security Architecture
  - **Threat Defense**
    - SECS99: Defending Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses | GCUX

### Specialized Penetration Testing

**Focused Techniques & Areas**

- **In-Depth Coverage**
  - **Vulnerability Assessment**
    - SECS60: Enterprise Threat and Vulnerability Assessment
  - **Networks**
    - SECS64: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GPNP
    - SECS66: Advanced Exploit Development for Penetration Testers
  - **Web Apps**
    - SECS57: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
  - **Mobile**
    - SECS75: Mobile Device Security and Ethical Hacking | GMOB
  - **Wireless**
    - SECS87: Wireless Penetration Testing and Ethical Hacking | GWRN
  - **Python Coding**
    - SECS73: Automating Information Security with Python | GMPC

### Digital Forensics, Malware Analysis, & Threat Intel

**Specialized Investigative Skills**

- **Malware Analysis**
  - FOR810: Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GREM
- **Threat Intelligence**
  - FOR815: Threat Intelligence | GCBI
- **Digital Forensics & Media Exploitation**
  - FOR857: Smartphone Forensic Analysis In-Depth | GASF
  - FOR26: Advanced Memory Forensics & Threat Detection
  - FOR150: Mac and iOS Forensic Analysis and Incident Response

### Advanced Management

**Advanced Leadership, Audit, Legal**

- **Management Skills**
  - MG520: Security Strategic Planning, Policy, and Leadership | GSTRY
  - MG525: IT Project Management, Effective Communication, and PMBOK Exam Prep | GPM
- **Audit & Legal**
  - MG528: Auditing & Monitoring Networks, Perimeters, and Systems | GSNM
  - MG821: Law of Data Security and Investigations | GLEG

### Industrial Control Systems

**ICS Security Professionals Need**

- **Essentials**
  - ICSS02: ICS/SCADA Security Essentials | GCSP
  - ICSS03: ICS Active Defense and Incident Response | GCSP
- **NERC Protection**
  - NERC Security Essentials: ICSS04 Essentials for NERC Critical Infrastructure Protection | GCSP

### Development & Secure Coding

**Every Developer Should Know**

- **Secure Web Apps**
  - DEV532: Defending Web Applications Security Essentials | GWEB
  - DEV540: Secure Web Apps and Cloud Application Security
- **Language-Specific Courses**
  - **JAVA/EE**
    - DEV541: Securing Coding in Java/EE: Developing Defensible Applications | GISP-JAVA
  - **NET**
    - DEV544: Securing Coding in .NET: Developing Defensible Applications | GISP-NET

See in-depth course descriptions and the digital version of this roadmap at: [www.sans.org/roadmap](http://www.sans.org/roadmap)

To learn more about additional SANS courses, go to: [www.sans.org/courses](http://www.sans.org/courses)
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
</tr>
<tr>
<td>SEC460</td>
<td>Enterprise Threat and Vulnerability Assessment <strong>NEW!</strong></td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis <strong>NEW!</strong></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits &amp; Incident Handling</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture <strong>NEW!</strong></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Implementing Kill Chain Defenses <strong>NEW!</strong></td>
</tr>
<tr>
<td>SEC617</td>
<td>Wireless Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation</td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
</tr>
<tr>
<td>SEC760</td>
<td>Advanced Exploit Development for Penetration Testers</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
</tr>
<tr>
<td>FOR527</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>FOR585</td>
<td>Advanced Smartphone Forensics</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Analysis Tools and Techniques</td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials For Managers <strong>NEW!</strong></td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
</tr>
<tr>
<td>ICS515</td>
<td>ICS Active Defense and Incident Response</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
</tr>
<tr>
<td>NETWARS</td>
<td>DFIR, Cyber Defence, Core</td>
</tr>
</tbody>
</table>

**2019 Event Schedule**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Course Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 Feb - 2 Mar</td>
<td>Tokyo</td>
<td>SEC401</td>
</tr>
<tr>
<td>9 Feb - 13 Jul</td>
<td>Tokyo</td>
<td>SEC401</td>
</tr>
<tr>
<td>30 Sep - 12 Oct</td>
<td>Tokyo</td>
<td>SEC401</td>
</tr>
<tr>
<td>25 Nov - 30 Nov</td>
<td>Tokyo</td>
<td>SEC401</td>
</tr>
<tr>
<td>28 Oct - 2 Nov</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>20 Jan - 24 Jan</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>21 Feb - 27 Feb</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>3 Mar - 9 Mar</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>27 Mar - 2 Apr</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>10 Apr - 16 Apr</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>19 Apr - 25 Apr</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>2 May - 8 May</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>11 May - 17 May</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>18 May - 24 May</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>25 May - 31 May</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>4 Jun - 10 Jun</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>11 Jun - 17 Jun</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>18 Jun - 24 Jun</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>25 Jun - 30 Jun</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>7 Jul - 12 Jul</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>13 Jul - 19 Jul</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>20 Jul - 26 Jul</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>27 Jul - 2 Aug</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>3 Aug - 9 Aug</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>10 Aug - 16 Aug</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>17 Aug - 23 Aug</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>24 Aug - 30 Aug</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>31 Aug - 6 Sep</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>7 Sep - 13 Sep</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>14 Sep - 20 Sep</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>21 Sep - 27 Sep</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>28 Sep - 4 Oct</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>5 Oct - 11 Oct</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>12 Oct - 18 Oct</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>26 Oct - 1 Nov</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>2 Nov - 8 Nov</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>9 Nov - 15 Nov</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>16 Nov - 22 Nov</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>23 Nov - 29 Nov</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>30 Nov - 6 Dec</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>7 Dec - 13 Dec</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>14 Dec - 20 Dec</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>21 Dec - 27 Dec</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
<tr>
<td>28 Dec - 3 Jan</td>
<td>Osaka</td>
<td>SEC401</td>
</tr>
</tbody>
</table>

Dates and locations may change – for complete up-to-date information, please visit [www.sans.org/security-training/bylocation](http://www.sans.org/security-training/bylocation)
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>City</th>
<th>Dates</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC401</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Manila</td>
<td>11-23 Mar</td>
<td>Philippines</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>8-20 Jul</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>14-26 Oct</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Singapore</td>
<td>18-23 Nov</td>
<td>Singapore</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>24 Jun - 1 Jul</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Melbourne</td>
<td>5-10 Aug</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Canberra</td>
<td>2-21 Sep</td>
<td>Australia</td>
</tr>
<tr>
<td>SEC504</td>
<td>Cyber Defence</td>
<td>Sydney</td>
<td>4-16 Nov</td>
<td>Australia</td>
</tr>
</tbody>
</table>
SANS Faculty

At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge through their own real-world examples and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 100 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organisations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organisations around the world.

In addition to their impressive résumés, every member of the SANS faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they’re present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you’ll be able to apply what you learn from these top-tier instructors as soon as you return to work.

“I have attended several SANS classes over the years and I am always impressed with the level of knowledge and professionalism of the instructors.”

- Ron Foupht, Sirius Computer Solutions

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

Is SEC401: Security Essentials Bootcamp Style the right course for you?

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, the SEC401 course will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

Learn to build a security roadmap that can scale today and into the future. 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.
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.

SEC504 helps you turn the tables on computer attackers by helping you understand attackers’ tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. This course 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.

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.

“The training offered at SANS is the best in the industry, and the SEC504 course is a must for any IT security professional – highly recommended.”

- Michael Hoffman, Shell Oil Products US
Intrusion Detection In-Depth

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.

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.

This course 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.

“"The labs were instrumental in reinforcing the instructor-led material, making it easier to grasp the concepts.”

-Richard Llanas, SSCLANT
We continue to underestimate the tenacity of our adversaries! Organisations are investing significant time and financial and human resources 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, which is 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!

“SEC511 was a wonderful look into the world of the ‘Blue Team.’ The authors really put together a robust course full of great ideas and tactics to take on intrusion detection and continuous monitoring.”

-Cameron Johns, Tyson Foods, Inc.
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

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

If you answer yes to any of these questions, the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cyber security that will serve as the foundation of your security 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 SANS course in this progression, 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.

“SANS instructors have an uncanny ability to take complex/complicated subject matter and distill it to terms easily understood by non-technical students.”

-F. Molinari, CitiBank

Who Should Attend
- Vulnerability assessors
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- System administrators

You Will Be Able To
- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilise built-in Windows tools to see your network settings
- Recognise and be able to discuss various security technologies, including anti-malware, firewalls, and intrusion detection systems, content filters, sniffers, etc.
- Build a simple but fully functional firewall configuration
- Secure your browser using a variety of security plug-ins
- Secure a wireless access point (also known as a wireless router)
- Scan for malware, clean malware from a system, and whitelist legitimate software identified by an anti-malware scanner as “potentially unwanted”
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

Live Training
See updated schedule at sans.org/apac

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
Immeasurable amounts of personal and potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update daily via their devices. Those data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

Many people think using their favorite Internet search engine is sufficient to find the data they need and do not realize that most of the Internet is not indexed by search engines. SEC487 teaches students legitimate and effective ways to find, gather, and analyze these data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the information, we’ll show you how to ensure that it is sound, how to analyze what you’ve gathered, and how to make it is useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. You will learn current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. More than 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

“Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!”

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

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

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 effective and robust preventive and detective measures, completing the security lifecycle.

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

You Will Be Able To
- Identify the threats against network infrastructures and build defensible networks that minimise the impact of attacks
- Access tools that can be used to analyse a network to prevent attacks and detect the adversary
- Decode and analyse packets using various tools to identify anomalies and improve network defences
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organisation to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process
- Use various tools to identify and remediate malware across your organisation
- Create a data classification program and deploy data loss prevention solutions at both a host and network level

Live Training
See updated schedule at sans.org/apac

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

“The labs were instrumental in reinforcing the instructor-led material, making it easier to grasp the concepts.”
-Richard Llanas, SSCLANT
16

Defensible Security Architecture  NEW!

SEC530: Defensible Security Architecture is designed to help students build and maintain a truly defensible security architecture. “The perimeter is dead” is a favorite saying in this age of mobile, cloud, and the Internet of Things, and we are indeed living in a new world of “de-perimeterisation” where the old boundaries of “inside” and “outside” or “trusted” and “untrusted” no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the “encrypt everything” mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better prevent the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, this course will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

You Will Learn To:

- Analyse a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Maximise the current investment by reconfiguring existing equipment to become more defensible
- Configure computer systems and network components to support proper logging and continuous monitoring
- Improve both preventive and detective capabilities
- Improve the security of devices from layer 1 (physical) through layer 7 (application)

“Every day of SEC530 has provided new insight and information. The labs are great, and I can’t wait to put it all together. No matter how experienced a professional you are, SANS always teaches you something new.”

-Ron Foupht, Sirius Computer Solutions
As more organisations 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.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We'll start with a brief introduction to cloud security fundamentals, 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 defence focal areas to the cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defence 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.

“SEC545 helped to better align our policies to include cloud systems, and it gave me more insight into cloud systems and their configurations.”

-Craig Lunde, Discovery Benefits Inc.
Many organisations have logging capabilities but lack the people and processes to analyse them. 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 students with the training, methods, and processes to enhance 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 SANS-sponsored free 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 class 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, how to 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.

“The immediate value of the course material is unlike any course or training I’ve received. A++”

-David Savercool, Cart Container
Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses

You just got hired to help our virtual organisation “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: "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.

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?

“SEC599 gives really good background about adversary behavior and the steps needed to detect it.”

-Tarot Wake, Halkyn Consulting Ltd
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.

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.

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 app manipulation, pivoting through the target environment to model the attacks of real-world bad guys to emphasise the importance of defence in depth.

“SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective.”

-Steve Nolan, General Dynamics
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.

“SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool, or that tool.”

-Christopher J. Stover, Infogressive Inc.
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.

Who Should Attend
- Vulnerability assessors
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- System administrators

“...of vulnerability management is process, and SEC460 shows process creation and improvement options.”
-Patrick O’Connell, Anixter, Inc.
Automating Information Security with Python

Who Should Attend

- Security professionals who benefit from automating routine tasks so they can focus on what’s most important
- Forensics analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evildoers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

You Will Be Able To

- Develop forensics tools to carve artifacts from forensics evidence for which no other tool exists or use third-party modules for well-known artifacts that hide evidence relevant to your investigations
- Create defensive tools to automate the analysis of log file and network packets using hunt team techniques to track down attackers in your network
- Implement custom whitelisting, blacklisting, signature detection, long-tail and short-tail analysis, and other data analysis techniques to find attacks overlooked by conventional methods
- Write penetration testing tools including several backdoors with features like process execution, upload and download payloads, port scanning and more
- Build essential tools that evade antivirus software and allow you to establish the required foothold inside your target

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 defences our organisations 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 defences 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 organisation big time. The answer is simple if you have the skills: Write a tool to automate your defences.

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 what is being taught. 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, customising, 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, organisations serious about security emphasise 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 weaponised.

“SEC573 is excellent. I went from having almost no python coding ability to being able to write functional and useful programs.”

-Caleb Jaren, Microsoft
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.
This course is designed for professionals seeking a comprehensive technical ability to understand, analyse, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entry points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organisations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, assess, and defend against these threats. These skills are “must-haves” for any high-performing security organisation.

For many analysts, “wireless” was once synonymous with “WiFi,” the ever-present networking technology, and many organisations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organisation. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device’s security for use within your organisation.

Beyond analysing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilised in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.
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.

This course offers 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.
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.

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

You Will Be Able To
- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 6-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse-engineer vulnerable code to write custom exploits

“No frills and goes right to the point. The first day alone is what other classes spend a full week on.”
-Michael Isbitski, Verizon Wireless

Live Training
See updated schedule at sans.org/apac

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.
Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organisations to significant attacks, undermining their defences when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SEC760: Advanced Exploit Development for Penetration Testers, the SANS Institute’s only 700-level course, teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyse patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

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

Course Author Statement

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

-Stephen Sims

“SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned.”

-Jenny Kitaichit, Intel
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 respond to real-world breach cases.

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

“FOR508 analyses Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!”

- Neel Mehta, Chevron
This course will enable you to 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: Threat Hunting, Analysis, and Incident Response 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.
Windows Forensic Analysis

Who Should Attend

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

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files

Live Training

See updated schedule at sans.org/apac

Online Training

OnDemand

Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

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 like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world’s best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can’t protect what you don’t understand, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn to recover, analyse, and authenticate forensic data on Windows systems. You’ll understand how to track detailed user activity on your network and how to 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 unimaginable 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 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out—attendees learn to analyse everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. This course utilises a brand-new intelligence property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analysing Windows systems. The detailed step-by-step workbook meticulously outlines the tools and techniques that each investigator should follow to solve a forensic case.

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

“Anyone involved in digital investigations needs to take this class! It covers or touches upon almost every aspect of Windows forensic investigations in a very short period of time.”

-Cy Bleistine, NJSP
Who Should Attend

- Security practitioners
- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Digital forensic analysts and malware analysts
- Federal agents and law enforcement officials
- Technical managers
- SANS alumni looking to take their analytical skills to the next level

Security practitioners should attend FOR578: Cyber Threat Intelligence because it is unlike any other technical training. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesise, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn about the different sources from which to collect adversary data and how to exploit and pivot off of those data
- Validate information received externally to minimise the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques that will complement their existing knowledge as well as establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary’s intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organisation. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organisations looking to establish or update their response and detection programs to deal with increasingly sophisticated 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.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries’ methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritise intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritisation and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organisation in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats.
SMARTPHONES HAVE MINDS OF THEIR OWN. DON’T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE AS USER ACTIVITY. IT’S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

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

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

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 20 hands-on labs that allow students to analyse different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

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

SMARTPHONE DATA CAN’T HIDE FOREVER – IT’S TIME TO OUTSMART THE MOBILE DEVICE!

“FOR585 helps you see evidence across multiple tools and see the strengths and weaknesses of each tool. This is extremely useful in the workplace.”

-Christine Oropeza, Stroz Friedberg
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 systematic 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.

“This is definitely one of those courses every professional working in the incident response should attend.”

-Kamal Ranjan, DarkMatter LLC
Security managers need both technical knowledge and management skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics.

This course empowers you to become an effective security manager and 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.

To accomplish this goal, MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues.

This approach prepares you to:

- Make sense of different cybersecurity frameworks
- Understand and analyse risk
- Understand the pros and cons of different reporting relationships
- Manage technical personnel
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud

MGT512 uses case studies, group discussions, team-based exercises, and in-class games to help students absorb both technical and management topics.

“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
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organisation than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

▌ **Develop Strategic Plans**
Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

▌ **Create Effective Information Security Policy**
Policy is a manager’s opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, “No way, I am not going to do that!” Policy must be aligned with an organisation’s culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organisation.

▌ **Develop Management and Leadership Skills**
Leadership is a capability that must be learned, exercised and developed to better ensure organisational success. Strong leadership is brought about primarily through selfless devotion to the organisation and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organisation’s mission. Learn to utilise management tools and frameworks to better lead, inspire, and motivate your teams.

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.
ICS/SCADA Security Essentials

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of 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 (ICS) 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 for industrial cybersecurity professionals

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

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. 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.

“I think having the GICSP certification is very meaningful in the line of work that I do and helps to establish credibility with our clients.”

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

This course will empower students to understand their networked industrial control system 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 an 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 by participating in labs and de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, 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.

“This course is the missing piece to get companies to take threats seriously, pursue the truth, and share their findings.”

-Rob Cantu, U.S. Department of Energy
Secure DevOps and Cloud Application Security

Who Should Attend
- Anyone working in the DevOps environment or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
- Anyone interested in learning how to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in learning how to leverage cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

Who Should Attend
Anyone working in the DevOps environment or transitioning to a DevOps environment
Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
Anyone interested in learning how to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS)
Anyone interested in learning how to leverage cloud application security services provided by AWS
Developers
Software architects
Operations engineers
System administrators
Security analysts
Security engineers
Auditors
Risk managers
Security consultants

You Will Be Able 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 workloads to the cloud
- Consume cloud services to secure cloud applications

Live Training
See updated schedule at sans.org/apac

Online Training
OnDemand
Complete this course anywhere, anytime, at your own pace, with four months of online access in the OnDemand platform.

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 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.

“SoE540 opened my eyes to a new way of thinking about operations and security unlike anything since SEC401: Security Essentials.”
-Todd Anderson, OBE
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
- System administrators
- Enterprise defenders
- Architects
- Network engineers
- Security operations specialists
- Incident responders
- Security analysts
- Security auditors
- Builders and breakers

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

The 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

40
SANS Flagship Programs and Free Resources

**GIAC Certifications**
SANS courses are the ideal preparation for a GIAC Certification, the highest standard in cybersecurity certification. More than 30 GIAC Certifications allow you to demonstrate your unique expertise in specialised areas of cybersecurity. No other certification program in the world comes close to GIAC in validating real-world knowledge and skill, due largely to the extensive exam preparation process and team of expert contributors. [www.giac.org](http://www.giac.org)

**SANS Technology Institute - Graduate Degrees and Certificates**
The graduate programs of the SANS Technology Institute are built upon proven SANS courses and certifications. Students can earn graduate degrees in Information Security Engineering or Information Security Management, or graduate certificates in Cybersecurity Engineering (Core), Cyber Defence Operations, Penetration Testing and Ethical Hacking, or Incident Response. [www.sans.edu](http://www.sans.edu)

**SANS CyberTalent**
- **Assessments**
  SANS offers six web-based assessment tools that give cybersecurity managers the information they need to better manage their team’s skills and performance, improve their hiring success rate, and make their training investment more productive.

- **Immersion Academies**
  SANS currently runs two training, certification, and employment academies for veterans and women, to fill the growing demand for new information security professionals with a qualified workforce that is skilled and prepared. [www.sans.org/cybertalent](http://www.sans.org/cybertalent)

**SANS Security Awareness**
Thousands of organisations with millions of employees use SANS Security Awareness as a first line of defence. Gartner’s magic quadrant analysis agrees. Protect your organisation from threats that target human vulnerabilities with security awareness training. SANS Security Awareness is expert-authored training, tools, and content for easy compliance, better behavior change, and a more secure culture. [www.sans.org/awareness](http://www.sans.org/awareness)

Join the SANS.org community today to enjoy these free resources at [www.sans.org/join](http://www.sans.org/join)

**SANS Webcasts**
Live, topical presentations from SANS experts, instructors, and trusted vendors

**SANS Posters**
Tools, tips and techniques to hang in your office

**Newsletters**
Three SANS e-newsletters, available for free

**Blogs**
Read what SANS instructors are thinking about in practice-area-specific blogs

**Tip of the Day**
Learn a new tip each day from the SANS Security Awareness team

**SANS Reading Room**
Constantly updated library of industry white papers

**20 Critical Controls**
Find supporting courses and case studies related to the critical security controls

**Internet Storm Center**
The Internet’s early warning system

**Security Policy Templates**
Build your own security policy using one of the provided templates
The SANS Asia-Pacific Team is ready to assist you

GENERAL INQUIRIES
AsiaPacific@sans.org

AUSTRALIA & NEW ZEALAND
+61 2 6198 3352
anz@sans.org

INDIA
+91 9741900324
india@sans.org

JAPAN
+81 3 3242 6276
japan@sans.org

SINGAPORE
+65 8612 5278
asiapacific@sans.org

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