Cybersecurity Training Roadmap

SANS’ comprehensive course offerings enable professionals to deepen their skills at every stage of their cybersecurity career.

Focus Job Roles
You are experienced in security, preparing for a specialized job role or focus

<table>
<thead>
<tr>
<th>Monitoring &amp; Detection</th>
<th>Intrusion Detection &amp; Monitoring Over Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Packets &amp; Networks</td>
<td>Intrusion Detection: SEC503 Intrusion Detection In-Depth</td>
</tr>
<tr>
<td>Monitoring &amp; Operations</td>
<td>SEC251 Continuous Monitoring and Security Operations</td>
</tr>
</tbody>
</table>

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 detect and deploy monitoring tools and to interpret their output.

Penetration Testing
Vulnerability Analysis & Ethical Hacking

Every Pen Tester Should Know
Networks: SEC506 Network Penetration Testing and Ethical Hacking | GROK
Web Apps: SEC542 Web-App Penetration Testing and Ethical Hacking | GWAPT

The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires different ways of thinking and different tools. Penetration testing skills are essential for defense specialists to improve their defenses.

Incident Response & Threat Hunting
Host & Network Forensics

Every Forensics and IT Professional Should Know
Endgame Forensics: FOR530 Windows Forensic Analysis | GCE
Network Forensics: FOR570 Advanced Network Forensics, Threat Hunting, Forensics, Analysis, and Incident Response | G4H

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.

Crucial Skills, Specialized Roles
You are a candidate for advanced or specialized training

Cyber Defense Operations

<table>
<thead>
<tr>
<th>Cyber Defense Operations</th>
<th>Hardened Specific Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue Team</td>
<td>SEC459 Blue Team Fundamentals: Security Operations and Analysis</td>
</tr>
<tr>
<td>OSINT</td>
<td>SEC469 Open Source Intelligence (OSINT) Gathering and Analysis</td>
</tr>
<tr>
<td>Advanced GSIS</td>
<td>SEC529 Advanced Security Essentials - Enterprise Defender</td>
</tr>
<tr>
<td>Windows/PowerShell</td>
<td>SEC526 Securing Windows and PowerShell Automation</td>
</tr>
<tr>
<td>Linux/Unix Defense</td>
<td>SEC506 Securing Linux/Unix</td>
</tr>
<tr>
<td>SWIM</td>
<td>SEC535 SWIM with Tactical Analytics</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>SEC510 Defensible Security Architecture and Engineering</td>
</tr>
<tr>
<td>Adversary Emulation</td>
<td>SEC599 Defending Advanced Adversaries - Purple Team Tactics and Kill Chain Defense</td>
</tr>
</tbody>
</table>

Specialized Penetration Testing

In-Depth Coverage
Vulnerability Assessments: SEC468 Enterprise and Cloud | Threat and Vulnerability Assessment | G3SA
Networks: SEC462 Advanced Penetration Testing, Exploit利用, and Ethical Hacking | GPNP
SEC461 Advanced Exploit Development for Penetration Testers
Web-Apps: SEC464 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques
Mobile: SEC525 Mobile Device Security and Ethical Hacking | GWROK
Cloud: SEC586 Cloud Penetration Testing
Web: SEC587 Wireless Penetration Testing and Ethical Hacking | GAWB
Python Coding: SEC571 Automating Information Security with Python | GPC
Adversary Emulation: SEC599 Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

Digital Forensics, Malware Analysis & Threat Intel
Specialized Investigations Skills

Essentials
Digital Forensics: FOR303 Digital Forensics Essentials
Malware Analysis: FOR305 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GSI
Threat Intelligence: FOR355 Cyber Threat Intelligence | GCTI
Digital Forensics & Media Exploitation: FOR405 Digital Forensics and Media Exploitation
Breach Forensics & Data Acquisition: FOR455 Breach Forensics & Data Acquisition | G1FA
Smartphone Analysis: FOR505 Smartphone Forensic Analysis In-Depth | GSAF
Memory Forensics: FOR515 Advanced Memory Forensics & Threat Detection
Mac Forensics: FOR516 Mac and iOS Forensic Analysis and Incident Response

Advanced Management

Advanced Leadership, Audit & Legal

Planning, Policy, Leadership: MOS750 Security Strategic Planning, Policy, and Leadership | G4TF
Project Management: MOS756 IT Project Management, Effective Communication, and PMI® Exam Prep | GSVN
Audit & Legal
Audit & Monitor: AUD500 Auditing and Monitoring Networks, Perimeters & Systems | GSVN
Law & Investigations: LEG501 Law of Data Security and Investigations | GEG

Industrial Control Systems

Every ICS Security Professional Should Know
Essentials: EC321 ICS/SCADA Security Essentials | GCEP
ICS Defense & Response: EC325 ICS Active Defense and Incident Response | GRD
ICS Advanced Security: EC326 ICS Cybersecurity In-Depth
MERP Protection: EC346 Essentials for MERP Critical Infrastructures Protection | GCP

Cloud Security
Every Cloud Security Ops Person Should Know
Essentials: EC348 Cloud Security Essentials | GCP
Secure DevOps: SEC505 Cloud Security and DevOps Automation | GSA
Cloud Pen Test: SEC508 Cloud Penetration Testing

To learn more about additional SANS courses, go to: sans.org/courses

See in-depth course descriptions and the digital version of this roadmap at: sans.org/roadmap

The most trusted source for cybersecurity training, certifications, degrees, and research

65+ hands-on courses
35+ certifications