Cybersecurity Training Roadmap

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

Focus Job Roles

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

Monitoring & Detection

- Intrusion Detection & Monitoring Over Time
  - Penetration Security: SECD04 Intrusion Detection - In-Depth | GCIA
  - Continuous Monitoring and Security Operations | GMC
  - 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 monitor threats and to interpret their output.

Penetration Testing

- Vulnerability Analysis & Ethical Hacking
  - Every Pen Tester Should Know
  - Networks: SECD80 Network Penetration Testing and Ethical Hacking | GMC
  - Web Apps: SECD42 Web-App Penetration Testing and Ethical Hacking | OMT
  - The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red and 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 Forensic and IR Professional Should Know
  - Endpoint Forensics: FOR500 Windows Forensic Analysis | GCIA
  - FOR546 Advanced Incident Response, Threat Hunting, and Digital Forensics | GMC
  - Network: FOR525 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GCIA
  - Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations require specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

Specialized Penetration Testing

- Focused Techniques & Areas
  - In-Depth Coverage
  - Vulnerability Assessment: SECD48 Enterprise Threat and Vulnerability Assessment | GMC
  - Networks: SECD80 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GMC
  - SECD95 Advanced Exploit Development for Penetration Testers
  - Web Apps: SECD42 Advanced Web-App Testing, Ethical Hacking, and Exploitation Techniques
  - Mobile: SECD78 Mobile Device Security and Ethical Hacking | GMC
  - Cloud: SECD88 Cloud Penetration Testing
  - Wireless: SECD97 Wireless Penetration Testing and Ethical Hacking | GAIN
  - Python Coding: SECD75 Automating Information Security with Python | GPC
  - Adversary Emulation: SECD98 Mobile Team Tactics - Adversary Emulation for Breach Prevention & Detection

Digital Forensics, Malware Analysis & Threat Intel

- Specialized Investigative Skills
  - Malware Analysis
  - Malware Analysis: FOR510 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GRS
  - Threat Intelligence
  - Cyber Threat Intelligence: FOR518 Cyber Threat Intelligence | GTE
  - Digital Forensics & Media Exploitation
  - Battlefield Forensics & Data Acquisition: FOR516 Battlefield Forensics & Data Acquisition
  - Smartphone Forensics: FOR515 Smartphone Forensics in Depth | GMC
  - Memory Forensics: FOR512 Advanced Memory Forensics & Threat Detection
  - Mac Forensics: FOR519 Mac and iOS Forensics Analysis and Incident Response

Advanced Management

- Advanced Leadership, Audit & Legal
  - Management, Bates
  - Planning, Policy Leadership: MGT414 Security Strategic Planning, Policy, and Leadership | GTRT
  - Managing Vulnerabilities: MGT414 Managing Security Vulnerabilities: Enterprise and Cloud
  - Project Management: MGT512 Project Management, Effective Communication, and PMB® Exam Prep | GCIA
  - Audit & Legal
  - Audit & Monitor: AUD507 Auditing and Monitoring Networks, Perimeters & Systems | GCIA
  - Law & Investigations: LEG503 Law of Data Security and Investigations | GCIA

Career Development Paths

You are a candidate for advanced or specialized training

Cyber Defense Operations

- Essential Specific Defenses
  - Specialized Defensive Area
  - Blue Team: SECD58 Blue Team Fundamentals: Security Operations and Analysis
  - Advanced Digital Forensics: SECD57 Advanced Digital Forensics | GMC
  - Defending Advanced Security Threats - Enterprise Defender | GCED
  - Windows/Server Security: SECD60 Securing Windows and Server Automation | GCOW
  - Linux/Unix Defense: SECD64 Securing Linux/Unix | GCIA
  - SRE: SECD59 SRE with Tactical Analytics | GCA
  - Other Advanced Defense Courses
    - Security Architecture: SECD54 Defensible Security Architecture and Engineering | GCIA
    - Security Leadership Essentials for Managers | GCIA
    - Security Controls: SECD52 Defending Advanced Adversaries - People, Team Tactics and Kill Chain Defenses | GAZ

Industrial Control Systems

- Every ICS Security Professional Should Know
  - Essentials: KS414 ICS/SCADA Security Essentials | GACP
  - ICS Defense & Response: KS315 ICS Active Defense and Incident Response | GRD
  - ICS Advanced Security: KS414 ICS Cybersecurity In-Depth
  - MER Capabilities
    - MER Security Essentials: KS446 Essentials for MER Critical Infrastructure Protection | GC-P

Cloud Security

- Every Developer Should Know
  - Secure Web-Apps: SECD22 Defending Web Applications Security Essentials | GRI
  - Secure DevOps: SECD24 Cloud Security and DevOps Automation | GCA
  - Cloud Security: SECD46 Cloud Security Architecture and Operations

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

SANS courses, go to sans.org/roadmap

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

65+ hands-on courses
35+ certifications