Cybersecurity Training Roadmap

Career Development Paths

SANS' 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 the areas of management, legal, and audit.

Baseline Skills

New to Cyber Security — Concepts, Terms & Skills

Cyber Security Fundamentals	SEC301 **Introduction to Cyber Security** | GISF

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

Core Techniques — Prevent, Defend & Maintain

Every Security Professional Should Know	
Security Essentials	SEC401 **Security Essentials Bootcamp Style** | GSEC
Hacker Techniques	SEC504 **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.

COURSE LISTING KEY:

Topic	Course Code	Course Title	GIAC Certification
Essentials	ICS410	**ICS/SCADA Security Essentials**	GICSP

Security Management — Managing Technical Security Operations

Every Security Manager Should Know	
Leadership Essentials	MGT512 **Security Leadership Essentials for Managers** | GSLC
Critical Controls	SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Focus Job Roles

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

Monitoring & Detection — Intrusion Detection & Monitoring Over Time

Scan Packets & Networks	
Intrusion Detection	SEC503 **Intrusion Detection In-Depth** | GCIA
Monitoring & Operations	SEC511 **Continuous Monitoring and Security Operations** | GMON

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

Every Pen Tester Should Know	
Networks	SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN
Web Apps	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT

The professional who can find weakness 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 IR Professional Should Know	
Endpoint Forensics	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA
Network Forensics	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

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.

CISSP® Training	MGT414 **SANS Training Program for CISSP® Certification** | GISP

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations — Harden Specific Defenses

Specialized Defensive Area	
Blue Team	SEC450 **Blue Team Fundamentals: Security Operations and Analysis**
OSINT	SEC487 **Open-Source Intelligence (OSINT) Gathering & Analysis** | GOSI
Advanced Generalist	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
Windows/Powershell	SEC505 **Securing Windows and PowerShell Automation** | GCWN
Linux/Unix Defense	SEC506 **Securing Linux/Unix** | GCUX
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
Other Advanced Defense Courses	
Security Architecture	SEC530 **Defensible Security Architecture and Engineering** | GDSA
Adversary Emulation	SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT

Specialized Penetration Testing — Focused Techniques & Areas

In-Depth Coverage	
Vulnerability Assessment	SEC460 **Enterprise Threat and Vulnerability Assessment** | GEVA
Networks	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC760 **Advanced Exploit Development for Penetration Testers**
Web Apps	SEC642 **Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques**
Mobile	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
Cloud	SEC588 **Cloud Penetration Testing**
Wireless	SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN
Python Coding	SEC573 **Automating Information Security with Python** | GPYC
Adversary Emulation	SEC699 **Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection**

Digital Forensics, Malware Analysis & Threat Intel — Specialized Investigative Skills

Malware Analysis	
Malware Analysis	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM
Threat Intelligence	
Cyber Threat Intelligence	FOR578 **Cyber Threat Intelligence** | GCTI
Digital Forensics & Media Exploitation	
Battlefield Forensics & Data Acquisition	FOR498 **Battlefield Forensics & Data Acquisition**
Smartphones	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
Memory Forensics	FOR526 **Advanced Memory Forensics & Threat Detection**
Mac Forensics	FOR518 **Mac and iOS Forensic Analysis and Incident Response**

Advanced Management — Advanced Leadership, Audit & Legal

Management Skills	
Planning, Policy, Leadership	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
Managing Vulnerabilities	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
Project Management	MGT525 **IT Project Management, Effective Communication, and PMP® Exam Prep** | GCPM
Audit & Legal	
Audit & Monitor	AUD507 **Auditing and Monitoring Networks, Perimeters & Systems** | GSNA
Law & Investigations	LEG523 **Law of Data Security and Investigations** | GLEG

Industrial Contol Systems

Every ICS Security Professional Should Know	
Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP
ICS Defense & Response	ICS515 **ICS Active Defense and Incident Response** | GRID
ICS Advanced Security	ICS612 **ICS Cybersecurity In-Depth**
NERC Protection	
NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

Cloud Security

Every Developer Should Know	
Secure Web Apps	SEC522 **Defending Web Applications Security Essentials** | GWEB
Secure DevOps	SEC540 **Cloud Security and DevOps Automation** | GCSA
Cloud Security	SEC545 **Cloud Security Architecture and Operations**

65+ hands-on courses

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

35+ certifications

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

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