Training Roadmap | Development Paths

Quick Summary | Course Code | Course Title | GIAC Certification

Example: Advanced Security Essentials — SEC501 Advanced Security Essentials - Enterprise Defender — GCED Certification

Baseline Skills

1 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 Certification
Hacker Techniques	SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	GCIH Certification

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 attackers 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.

New to Cybersecurity	SEC301	Intro to Information Security	GISF Certification

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

Security Management *Managing Technical Security Operations*

Every Security Manager Should Know

Leadership Essentials	MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	GSLC Certification
Critical Controls	SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	GCCC Certification

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

2 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 Certification
Monitoring & Operations	SEC511	Continuous Monitoring and Security Operations	GMON Certification

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 Certification
Web Apps	SEC542	Web App Penetration Testing and Ethical Hacking	GWAPT Certification

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 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 and IR Professional Should Know

Endpoint Forensics	FOR500	Windows Forensics	FOR508	Adv. Incident Response & Threat Hunting	GCFE | GCFA Certifications
Network Forensics	FOR572	Advanced Network Forensics and Analysis			GNFA Certification

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 Certification

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.

3 You are a candidate for specialized or advanced training

Cyber Defense Operations *Harden Specific Defenses*

Specialized Defensive Area

Advanced Generalist	SEC501	Advanced Security Essentials – Enterprise Defender	GCED Certification
Cloud Security	SEC545	Cloud Security Architecture and Operations	
Windows/ Powershell	SEC505	Securing Windows and PowerShell Automation	GCWN Certification
Linux/ Unix Defense	SEC506	Securing Linux/Unix	GCUX Certification
Virtualized Data Centers	SEC579	Virtualization and Software-Defined Security	
SIEM	SEC555	SIEM with Tactical Analytics	

Other Advanced Defense Courses

Critical Controls	SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	GCCC Certification
Threat Defense	SEC599	Defeating Advanced Adversaries -Implementing Kill Chain Defenses	

Advanced Penetration Testing *Advanced Techniques & Areas*

In-Depth Coverage

Networks	SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GXPN Certification
	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 Certification
Wireless	SEC617	Wireless Penetration Testing and Ethical Hacking	GAWN Certification

Other Advanced Pen Testing Courses

Hands-On Ranges	SEC561	Immersive Hands-on Hacking Techniques	
	SEC562	CyberCity Hands-on Kinetic Cyber Range Exercise	
Python for Pen Testers	SEC573	Automating Information Security with Python	GPYC Certification

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

Malware Analysis

Malware Analysis	FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	GREM Certification

Threat Intelligence

Cyber Threat Intelligence	FOR578	Cyber Threat Intelligence	GCTI Certification

Digital Forensics & Media Exploitation

Smartphones	FOR585	Advanced Smartphone Forensics	GASF Certification
Memory Forensics	FOR526	Memory Forensics In-Depth	
Mac Forensics	FOR518	Mac Forensic Analysis	

Advanced Management *Advanced Leadership, Audit, Legal*

Management Skills

Planning, Policy, Leadership	MGT514	IT Security Strategic Planning, Policy, and Leadership	GSTRT Certification
Managing Operations	MGT517	Managing Security Operations: Detection, Response, and Intelligence	
Project Management	MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep	GCPM Certification

Audit & Legal

Audit & Monitor	AUD507	Auditing and Monitoring Networks, Perimeters & Systems	GSNA Certification
Law & Investigations	LEG523	Law of Data Security and Investigations	GLEG Certification

Development & Secure Coding

Every Developer Should Know

Secure Web Apps	DEV522	Defending Web Applications Security Essentials	GWEB Certification
Secure DevOps	DEV540	Secure DevOps and Cloud Application Security	

Language-Specific Courses

JAVA/JEE	DEV541	Secure Coding in Java/JEE: Developing Defensible Applications	GSSP-JAVA Certification
.NET	DEV544	Secure Coding in .NET: Developing Defensible Applications	GSSP-.NET Certification

Industrial Control Systems

ICS Security Professionals Need

Essentials	ICS410	ICS/SCADA Security Essentials	GICSP Certification
ICS Defense & Response	ICS515	ICS Active Defense and Incident Response	GRID Certification

NERC Protection

NERC Security Essentials	ICS456	Essentials for NERC Critical Infrastructure Protection	GCIP Certification