Training Roadmap | Development Paths

Key: Topic | Course Code | GIAC Certification
Advanced Generalist SEC**501** Advanced Security Essentials – Enterprise Defender | **GCED**
Course Title

Baseline Skills

Focus Job Roles

Crucial Skills, Advanced, or Specialized Roles

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 management, legal, and audit.

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	SEC**401** Security Essentials Bootcamp Style | **GSEC**
Hacker Techniques	SEC**504** 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 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	SEC**301** Introduction to Cyber Security | **GISF**

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	SEC**503** Intrusion Detection In-Depth | **GCIA**
Monitoring & Operations	SEC**511** 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	SEC**560** Network Penetration Testing and Ethical Hacking | **GPEN**
Web Apps	SEC**542** 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 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	FOR**500** Windows Forensic Analysis | **GCFE**	FOR**508** Advanced Digital Forensics, Incident Response, and Threat Hunting | **GCFA**
Network Forensics	FOR**572** 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.

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	MGT**512** Security Leadership Essentials for Managers | **GSLC**
Critical Controls	SEC**566** 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.

CISSP® Training	MGT**414** SANS Training Program for CISSP® Certification | **GISP**

3 **You are a candidate for specialized or advanced training**

Cyber Defense Operations | Harden Specific Defenses

Specialized Defensive Area	
Advanced Generalist	SEC**501** Advanced Security Essentials – Enterprise Defender | **GCED**
Cloud Security	SEC**545** Cloud Security Architecture and Operations
Windows/ Powershell	SEC**505** Securing Windows and PowerShell Automation | **GCWN**
Linux/ Unix Defense	SEC**506** Securing Linux/Unix | **GCUX**
Virtualized Data Centers	SEC**579** Virtualization and Software-Defined Security
SIEM	SEC**555** SIEM with Tactical Analytics | **GCDA**
Other Advanced Defense Courses	
Critical Controls	SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
Security Architecture	SEC**530** Defensible Security Architecture
Threat Defense	SEC**599** Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses | **GDAT**

Specialized Penetration Testing | Focused Techniques & Areas

In-Depth Coverage	
Vulnerability Assessment	SEC**460** Enterprise Threat and Vulnerability Assessment
Networks	SEC**660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN** SEC**760** Advanced Exploit Development for Penetration Testers
Web Apps	SEC**642** Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques
Mobile	SEC**575** Mobile Device Security and Ethical Hacking | **GMOB**
Wireless	SEC**617** Wireless Penetration Testing and Ethical Hacking | **GAWN**
Hands-On Ranges	SEC**562** CyberCity Hands-on Kinetic Cyber Range Exercise
Python Coding	SEC**573** Automating Information Security with Python | **GPYC**

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

Malware Analysis	
Malware Analysis	FOR**610** Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM**
Threat Intelligence	
Cyber Threat Intelligence	FOR**578** Cyber Threat Intelligence | **GCTI**
Digital Forensics & Media Exploitation	
Smartphones	FOR**585** Advanced Smartphone Forensics | **GASF**
Memory Forensics	FOR**526** Memory Forensics In-Depth
Mac Forensics	FOR**518** Mac Forensic Analysis

Advanced Management | Advanced Leadership, Audit, Legal

Management Skills	
Planning, Policy, Leadership	MGT**514** Security Strategic Planning, Policy, and Leadership | **GSTRT**
Project Management	MGT**525** IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM**
Audit & Legal	
Audit & Monitor	AUD**507** Auditing and Monitoring Networks, Perimeters & Systems | **GSNA**
Law & Investigations	LEG**523** Law of Data Security and Investigations | **GLEG**

Industrial Control Systems

ICS Security Professionals Need	
Essentials	ICS**410** ICS/SCADA Security Essentials | **GICSP**
ICS Defense & Response	ICS**515** ICS Active Defense and Incident Response | **GRID**
NERC Protection	
NERC Security Essentials	ICS**456** Essentials for NERC Critical Infrastructure Protection | **GCIP**

Development & Secure Coding

Every Developer Should Know	
Secure Web Apps	DEV**522** Defending Web Applications Security Essentials | **GWEB**
Secure DevOps	DEV**540** Secure DevOps and Cloud Application Security
Language-Specific Courses	
JAVA/JEE	DEV**541** Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA**
.NET	DEV**544** Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET**