Cybersecurity Training Roadmap

Topic — Course Code — GIAC Certification

Essentials ICS410 **ICS/SCADA Security Essentials** | GICSP

Course Title

Baseline Skills

NEW TO CYBER SECURITY | COMPUTERS, TECHNOLOGY, & SECURITY

COMPUTER & IT FUNDAMENTALS	SEC275 **Foundations: Computers, Technology & Security** | GFACT
CYBER SECURITY FUNDAMENTALS	SEC301 **Introduction to Cyber Security** | GISF

This entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.

CORE TECHNIQUES | PREVENT, DEFEND, MAINTAIN

Every Security Professional Should Know

SECURITY ESSENTIALS	SEC401 **Security Essentials: Network, Endpoint & Cloud** | GSEC

Whether you are new to information security or a seasoned practitioner with a specialized focus, SEC401 will provide the essential information security skills and techniques you need to protect and secure your critical information and technology assets, whether on-premise or in the cloud.

BLUE TEAM	SEC450 **Blue Team Fundamentals: Security Operations and Analysis** | GSOC
ATTACKER TECHNIQUES	SEC504 **Hacker Tools, Techniques, 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.

FORENSICS ESSENTIALS

Every Forensics and IR Professional Should Know

FORENSICS ESSENTIALS	FOR308 **Digital Forensics Essentials**
BATTLEFIELD FORENSICS & DATA ACQUISITION	FOR498 **Battlefield Forensics & Data Acquisition** | GBFA

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Professional Should Know

ESSENTIALS	ICS410 **ICS/SCADA Security Essentials** | GICSP

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Manager Should Know

ESSENTIALS	ICS418 **ICS Security Essentials for Managers**

CLOUD SECURITY ESSENTIALS

Every Cloud Security Professional Should Know

ESSENTIALS	SEC488 **Cloud Security Essentials** | GCLD
DEVSECOPS	SEC534 **Secure DevOps: A Practical Introduction**

If you are new to cybersecurity or looking to up-skill, cloud security essentials is a requirement for today's organizations. These courses provide the basic knowledge required to introduce students to the cloud security industry, as well as in-depth, hands-on practice in labs.

Focused Job Roles

DESIGN, DETECTION, AND DEFENSIVE CONTROLS

Focused Cyber Defense Skills

ADVANCED GENERALIST	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
MONITORING & OPERATIONS	SEC511 **Continuous Monitoring and Security Operations** | GMON
SECURITY ARCHITECTURE	SEC530 **Defensible Security Architecture and Engineering** | GDSA

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.

Open-Source Intelligence

OSINT	SEC487 **Open-Source Intelligence (OSINT) Gathering and Analysis** | GOSI

OFFENSIVE OPERATIONS | VULNERABILITY ANALYSIS, PENETRATION TESTING

Every Offensive Professional Should Know

NETWORK PEN TESTING	SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN
WEB APPS	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT
VULNERABILITY ASSESSMENT	SEC460 **Enterprise and Cloud | Threat and Vulnerability Assessment** | GEVA

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. Offensive skills are essential for cybersecurity professionals 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 FOR608 **Enterprise-Class Incident Response & Threat Hunting**
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.

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Professional Should Know

ICS DEFENSE & RESPONSE	ICS515 **ICS Visibility, Detection, and Response** | GRID
ICS ADVANCED SECURITY	ICS612 **ICS Cybersecurity In-Depth**
NERC Protection	
NERC SECURITY ESSENTIALS	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

CORE CLOUD SECURITY

Preparation for More Focused Job Functions

PUBLIC CLOUD	SEC510 **Public Cloud Security: AWS, Azure, and GCP** | GPCS
SECURE APPS & APIS	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
AUTOMATION & DEVSECOPS	SEC540 **Cloud Security and DevSecOps Automation** | GCSA

With the massive global shift to the cloud, it becomes more critical for every organization to have experts who understand the security risks and benefits that come with public cloud use, how to navigate and take full advantage of multicloud environments, and how to incorporate security from the start of all development projects.

Specific Skills, Specialized Roles

ADVANCED CYBER DEFENSE | HARDEN SPECIFIC DEFENSES

Platform Focused	
WINDOWS/ POWERSHELL	SEC505 **Securing Windows and PowerShell Automation** | GCWN
Topic Focused	
TRAFFIC ANALYSIS	SEC503 **Intrusion Detection In-Depth** | GCIA
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
POWERSHELL	SEC586 **Blue Team Operations: Defensive PowerShell**
PYTHON CODING	SEC573 **Automating Information Security with Python** | GPYC
DATA SCIENCE	SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals**

Open-Source Intelligence

OSINT	SEC587 **Advanced Open-Source Intelligence (OSINT) Gathering and Analysis**

SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

Network, Web & Cloud	
EXPLOIT DEVELOPMENT	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC661 **ARM Exploit Development** SEC760 **Advanced Exploit Development for Penetration Testers**
WEB APPS	SEC642 **Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**
CLOUD PEN TEST	SEC588 **Cloud Penetration Testing** | GCPN
Specialized Penetration Testing	
SOCIAL ENGINEERING	SEC467 **Social Engineering for Security Professionals**
ACTIVE DEFENSE	SEC550 **Cyber Deception - Attack Detection, Disruption and Active Defense**
BLOCKCHAIN	SEC554 **Blockchain and Smart Contract Security**
RED TEAM	SEC564 **Red Team Exercises and Adversary Emulation**
MOBILE	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
PEN TEST	SEC580 **Metasploit Kung Fu for Enterprise Pen Testing**
WIRELESS	SEC556 **IoT Penetration Testing** SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN
Purple Team	
ADVERSARY EMULATION	SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT SEC699 **Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection**

DIGITAL FORENSICS, MALWARE ANALYSIS, & THREAT INTELLIGENCE | SPECIALIZED INVESTIGATIVE SKILLS

Specialization	
CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics and Incident Response**
MALWARE ANALYSIS	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM FOR710 **Reverse-Engineering Malware: Advanced Code Analysis**
Threat Intelligence	
CYBER THREAT INTELLIGENCE	FOR578 **Cyber Threat Intelligence** | GCTI
Digital Forensics & Media Exploitation	
SMARTPHONES	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
MAC FORENSICS	FOR518 **Mac and iOS Forensic Analysis and Incident Response**

ADVANCED CLOUD SECURITY

Specialization for Advanced Skills & Roles

CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics and Incident Response**
MONITORING & DETECTION	SEC541 **Cloud Security Monitoring and Threat Detection**
CLOUD PEN TEST	SEC588 **Cloud Penetration Testing** | GCPN

Learning how to convert traditional cybersecurity skills into the nuances of cloud security is a necessity for proper monitoring, detection, testing, and defense.

CLOUD CYBERSECURITY LEADERSHIP AND GOVERNANCE

Every Cloud Security Leader Should Know

AUTOMATION & COMPLIANCE	SEC557 **Continuous Automation for Enterprise and Cloud Compliance**
VULNERABILITY MANAGEMENT	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
DESIGN & IMPLEMENTATION	MGT520 **Leading Cloud Security Design and Implementation**

FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know

CISSP® TRAINING	MGT414 **SANS Training Program for CISSP® Certification** | GISP
RISK MANAGEMENT	MGT415 **A Practical Introduction to Cyber Security Risk Management**
SECURITY AWARENESS	MGT433 **Managing Human Risk: Mature Security Awareness Programs**
CIS Controls	SEC440 **CIS Critical Controls: A Practical Introduction**

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those leaders 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.

CORE LEADERSHIP

Transformational Cybersecurity Leader	
TECHNOLOGY LEADERSHIP	MGT512 **Security Leadership Essentials for Managers** | GSLC
SECURITY STRATEGY	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
SECURITY CULTURE	MGT521 **Leading Cybersecurity Change: Building a Security-Based Culture**
Operational Cybersecurity Executive	
VULNERABILITY MANAGEMENT	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
SOC	MGT551 **Building and Leading Security Operations Centers** | GSOM
CRITICAL CONTROLS	SEC566 **Implementing and Auditing CIS Critical Controls** | GCCC

LEADERSHIP SPECIALIZATIONS

Cloud Cybersecurity Leadership	
VULNERABILITY MANAGEMENT	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
DESIGN & IMPLEMENTATION	MGT520 **Leading Cloud Security Design and Implementation**
AUTOMATION & COMPLIANCE	SEC557 **Continuous Automation for Enterprise and Cloud Compliance**
Management Specialization	
AUDIT & MONITOR	AUD507 **Auditing and Monitoring Networks, Perimeters & Systems** | GSNA
LAW & INVESTIGATIONS	LEG523 **Law of Data Security and Investigations** | GLEG
PROJECT MANAGEMENT	MGT525 **Managing Cybersecurity Initiatives & Effective Communication** | GCPM

SANS | GIAC CERTIFICATIONS

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

V1-12-2022