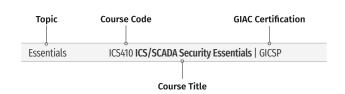
SANS Training Roadmap



Baseline Skills

Focused Job Roles

Specific Skills, Specialized Roles

NEW TO CYBERSECURITY | COMPUTERS, TECHNOLOGY, AND SECURITY

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

These entry-level courses cover a wide spectrum of security topics and are liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes these course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.

DESIGN, DETECTION, AND DEFENSIVE CONTROLS

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

Zero Trust for the Hybrid Enterprise | GDSA

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requ increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Open-Source Intelligence

Every Offensive Professional Should Know

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

ADVANCED CYBER DEFENSE | HARDEN SPECIFIC DEFENSES SEC505 Securing Windows and PowerShell Automation | GCWN POWERSHEL Topic-Focused SEC503 Intrusion Detection In-Denth | GCIA TRAFFIC ANALYSIS SIEM SEC555 SIEM with Tactical Analytics | GCDA POWERSHELL SEC586 Blue Team Operations: Defensive PowerShell PYTHON CODING SEC573 Automating Information Security with Python | GPYC SEC595 Applied Data Science and Machine Learning for Cybersecurity Professionals DATA SCIENCE

CORE TECHNIQUES | PREVENT, DEFEND, MAINTAIN

SEC401 Security Essentials: Network, Endpoint, and 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 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.

OFFENSIVE OPERATIONS | VULNERABILITY ANALYSIS, PENETRATION TESTING

SEC560 Enterprise Penetration Testing | GPEN SEC542 Web App Penetration Testing and Ethical Hacking | GWAPT 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.

SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

SEC587 Advanced Open-Source Intelligence (OSINT) Gathering & Analysis

Network, Web & Cloud SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GXPN SEC661 ARM Exploit Development EXPLOIT DEVELOPMENT

SEC760 Advanced Exploit Develop ment for Penetration Testers SEC588 Cloud Penetration Testing | GCPN CLOUD PEN TEST

Specialized Penetration Testing SOCIAL ENGINEERING SEC467 Social Engineering for Security Professionals ACTIVE DEFENSE ${\tt SEC550}\ \textbf{Cyber Deception - Attack Detection, Disruption \& Active Defense}$ BLOCKCHAIN SEC554 Blockchain and Smart Contract Security

SEC565 Red Team Operations and Adversary Emulation SEC670 Red Team Operations – Developing Custom Tools for Windows MOBILE SEC575 Mobile Device Security and Ethical Hacking | GMOB PEN TEST SEC580 Metasploit for Enterprise Penetration Testing SEC556 IoT Penetration Testing WIRELESS SEC617 Wireless Penetration Testing and Ethical Hacking | GAWN

SEC598 Security Automation for Offense, Defense, and Cloud SEC599 Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses | GDAT ADVERSARY EMULATION SEC699 Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection

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

FORENSICS ESSENTIALS

Every Forensics and IR Professional Should Know

FORENSICS ESSENTIALS FOR498 Battlefield Forensics & Data Acquisition | GBFA

INCIDENT RESPONSE & THREAT HUNTING | HOST & NETWORK FORENSICS

Every Forensics and IR Professional Should Know

FOR500 Windows Forensic Analysis | GCFE ENDPOIN1 and Digital Forensics | GCFA **FORENSICS** FOR532 Enterprise Memory Forensics In-Depth FOR608 Enterprise-Class Incident Response & 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

CLOUD FORENSICS FOR509 Enterprise Cloud Forensics & Incident Response | GCFR RANSOMWARE **FOR528 Ransomware for Incident Responders** FOR610 Reverse-Engineering Malwar Malware Analysis Tools and Techniques | GREM FOR710 Reverse-Engineering Malware: Advanced Code Analysis MALWARE ANALYSIS Threat Intelligence

FOR578 **Cyber Threat Intelligence** | GCTI FOR589 **Cybercrime Intelligence** CYBER THREAT INTELLIGENCE

Digital Forensics & Media Exploitation **SMARTPHONES** FOR585 Smartphone Forensic Analysis In-Depth | GASF FOR518 Mac and iOS Forensic Analysis and MAC FORENSICS

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Professional Should Know

ICS410 ICS/SCADA Security Essentials | GICSP

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Professional Should Know

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

Every ICS Security Manager Should Know

ESSENTIALS

CLOUD SECURITY ESSENTIALS

Every Cloud Security Professional Should Know

ICS418 ICS Security Essentials for Managers

CORE CLOUD SECURITY

Preparation for More Focused lob Functions

SEC510 Public Cloud Security: AWS, Azure, and GCP | GPCS SEC540 Cloud Security and DevSecOps Automation | GCSA & DEVSECOPS MONITORING SEC541 Cloud Security Attacker Techniques, Monitoring & Threat Detection ARCHITECTURE SEC549 Enterprise Cloud Security Architecture

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.

SPECIALIZATION IN CLOUD SECURITY

Specialization for Advanced Skills & Roles ΔΡΡΙ ΙΟΔΤΙΟΝ SEC522 Application Security: Securing Web Apps, APIs, and Microservices

SEC557 Cloud Security Continuous Compliance SEC588 Cloud Penetration Testing | GCPN CLOUD FORENSICS FOR509 Enterprise Cloud Forensics and Incident Response Learning how to convert traditional cybersecurity skills into the nuances of cloud security is a necessity for proper monitoring, detection, testing, and defense

CLOUD FUNDAMENTALS

Built for professionals who need to be conversant in basic cloud security concepts, principles, and terms, but who don't need "deep in the weeds" detail

SEC488 Cloud Security Essentials | GCLD 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

SEC388 Intro to Cloud Computing and Security

Every Cloud Security Leader Should Know

MGT516 Managing Security Vulnerabilities: Enterprise and Cloud DESIGN & MGT520 Leading Cloud Security Design and Implementation

FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know

CISSP® TRAINING MGT414 SANS Training Program for CISSP® Certification | GISP MGT415 A Practical Introduction to Cyber Security Risk Management MANAGEMENT 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 MGT512 Security Leadership Essentials for Managers | GSLC

BUSINESS LEADERSHIP & MANAGEMENT

| LEADERSHIP | Mo1312 Security Leadership Essentials for Managers 63Ec | |
|-------------------------------------|--|--|
| 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 | |
| | | |

SEC566 Implementing and Auditing Security Frameworks & Controls | GCCC

CTF & TRIVIA Bootup CTF SKILLS ASSESSMENT

These cyber range offerings cover the broadest range of topics

and are meant for all infosec professionals at all levels.

CYBER DEFENSE Netwars Cyber Defense DIGITAL FORENSICS & INCIDENT RESPONSE Netwars DFIR INDUSTRIAL CONTROL SYSTEMS Netwars ICS POWER GENERATION AND DISTRIBUTION Netwars GRID

Cvber42

SANS offers specialized versions of Netwars for more specific job roles. These cyber ranges dive deeper into the respective topics and help advance your career with situation-based challenges and scenarios rooted in real-life events.

LEADERSHIP SPECIALIZATIONS Cloud Cybersecurity Leadership

VIII NERABILITY

| MANAGEMENT | MGT516 Managing Security Vulnerabilities: Enterprise and Cloud | |
|----------------------------|---|--|
| DESIGN & IMPLEMENTATION | MGT520 Leading Cloud Security Design and Implementation | |
| 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 | |
| INCIDENT RESPONSE | MGT553 Cyber Incident Management | |
| | | |