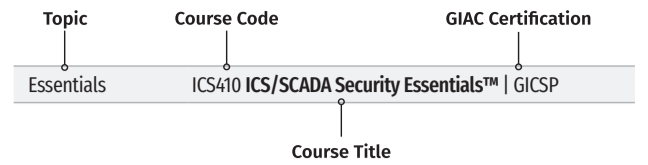


SANS Training Roadmap



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
Designed with beginners in mind, our foundations course covers essential concepts like operating systems, networking, security principles, and hands-on skills with tools used by professionals in the field.	
CYBERSECURITY FUNDAMENTALS	SEC301 Introduction to Cyber Security™ GISF
SEC301 introduces cybersecurity fundamentals for professionals who need to understand security without becoming technical practitioners. The course focuses on risk, trust, and decision-making, helping learners see how everyday actions influence security outcomes.	

CORE TECHNIQUES | PREVENT, DEFEND, MAINTAIN

SECURITY ESSENTIALS	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 SOC Analyst Training – Applied Skills for Cyber Defense Operations™ 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.	

ROLE-BASED TRAINING FROM SANS WORKFORCE SECURITY & RISK

Security Essentials for IT Administrators	
Role-based PCI DSS Compliance Training	
Protecting against cyber threats require continuous investment in skills development. Short-form modular training provides various teams with a role-focused understanding of evolving security concepts.	

FORENSICS ESSENTIALS

DIGITAL ACQUISITION AND RAPID TRIAGE	FOR498 Digital Acquisition and Rapid Triage™ GBFA
--------------------------------------	---

TACTICAL CLOUD DEFENSE

Cloud Security for Developers	
AWS	SEC480 AWS Secure Builder™ AWS Secure Builder Micro-Credential by GIAC
TACTICAL	SEC502 Cloud Security Tactical Defense™ GCLD
Applied skills for securing modern cloud workloads, blending security strategies with developer-focused practices to counter real-world threats.	

ROLE-BASED TRAINING FROM SANS WORKFORCE SECURITY & RISK

Web Application Security Training	
Progressive training paths geared towards all involved in the development process. Create a secure culture and ecosystem to mitigate vulnerabilities in critical web applications.	

INDUSTRIAL CONTROL SYSTEMS SECURITY

FOUNDATIONS	ICS310 ICS Cybersecurity Foundations™
ESSENTIALS	ICS410 ICS/SCADA Security Essentials™ GICSP
MANAGEMENT	ICS418 ICS Security Essentials for Leaders™

FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know	
CISSP® TRAINING	LDR414 SANS Training Program for CISSP® Certification™ GISP
SECURITY AWARENESS	LDR433 Managing Human Risk™ SSAP
CISSP-aligned security knowledge and human risk leadership skills enable emerging leaders to transition from technical execution to strategic leadership.	

SECURITY AWARENESS TRAINING FROM SANS WORKFORCE SECURITY & RISK

EndUser Awareness Training	
Engaging, modular, and multilingual end-user training focuses on the most pressing risk and compliance topics to address employee security behaviors and develop a culture of security across your organization.	

CYBER RANGES

MULTI-SKILL MULTI-DISCIPLINE	BootUp CTF Core NetWars SANS Skills Quest by NetWars
SANS Cyber Ranges provide interactive hands-on exercises that cover a wide range of topics to solidify skills and create muscle memory.	

ARTIFICIAL INTELLIGENCE

AI Security Essentials	
LEADERSHIP	AIS247 AI Security Essentials for Business Leaders™
THREAT HUNTING & DEFENSE	SEC595 Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™ GMLE
APPLICATION SECURITY	SEC495 Leveraging LLMs: Building & Securing RAG, Contextual RAG, and Agentic RAG™ SEC545 GenAI and LLM Application Security™
DIGITAL FORENSICS & INCIDENT RESPONSE	FOR563 Applied AI for Digital Forensics and Incident Response: Leveraging Local Large Language Models™

ROLE-BASED TRAINING FROM SANS WORKFORCE SECURITY & RISK

Workforce Risk Management Fundamentals for AI	
Designed for employees across all roles—from marketing to developers—this training prepares your team to adopt and use AI technologies safely and effectively.	

DESIGN, DETECTION, AND DEFENSIVE CONTROLS

Artificial Intelligence	
GenAI and LLM Defense	SEC411 AI Security Principles and Practices: GenAI and LLM Defense™
Focused Cyber Defense Skills	
ADVANCED GENERALIST	SEC501 Advanced Security Essentials – Enterprise Defender™ GCED
MONITORING & OPERATIONS	SEC511 Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ GMON
SECURITY ARCHITECTURE	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 requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.	
Open-Source Intelligence	
OSINT	SEC497 Practical Open-Source Intelligence (OSINT)™ GOSI

OFFENSIVE OPERATIONS | PENETRATION TESTING, OFFENSIVE SECURITY

Every Offensive Professional Should Know	
ENTERPRISE	SEC560 Enterprise Penetration Testing™ GPEN
RED TEAM	SEC565 Red Team Operations and Adversary Emulation™ GRTP
WEB APPS	SEC542 Web App Penetration Testing and Ethical Hacking™ GWAPT
EXPLOIT DEVELOPMENT	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™ GXPEN
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

ENDPOINT FORENSICS	FOR500 Windows Forensic Analysis™ GCFE FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics™ GCFA FOR608 Enterprise-Class Incident Response & Threat Hunting™ GEIR
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.

CORE CLOUD SECURITY

Preparation for More Focused Job Functions	
PREVENTION	SEC510 Cloud Security Engineering and Controls™ GPCS
AUTOMATION & DEVSECOPS	SEC540 Cloud Native Security and DevSecOps Automation™ GCSA
MONITORING & DETECTION	SEC541 Cloud Security Threat Detection™ GCTD
ARCHITECTURE	SEC549 Cloud Security Architecture™ GCAD

As cloud adoption becomes essential to modern enterprises, core cloud security capabilities are no longer optional. Build expertise across prevention, automation, monitoring and detection, and architecture, enabling organizations to operate in complex multicloud environments.

INDUSTRIAL CONTROL SYSTEMS SECURITY

DEFENSE & RESPONSE	ICS515 ICS Visibility, Detection, and Response™ GRID ICS612 ICS Cybersecurity In-Depth™
OFFENSIVE SECURITY	ICS613 ICS/OT Penetration Testing & Assessments™
NERC Protection	
NERC SECURITY ESSENTIALS	ICS456 Essentials for NERC Critical Infrastructure Protection™ GCIP

Industrial systems run the world, and the need for cybersecurity professionals to defend them is critical. Learn the skills needed to safeguard industrial environments for the sake of operations, national security, and the safety of human life.

CISO-LEVEL LEADERSHIP

Transformational Cybersecurity Leader	
TECHNOLOGY LEADERSHIP	LDR512 Security Leadership Essentials for Managers™ GSLC
SECURITY STRATEGY	LDR514 Security Strategic Planning, Policy, and Leadership™ GSTRT
SECURITY CULTURE	LDR521 Security Culture for Leaders™
Operational Cybersecurity Executive	
VULNERABILITY MANAGEMENT	LDR516 Strategic Vulnerability and Threat Management™
SOC	LDR551 Building and Leading Security Operations Centers™ GSOM
CIS CONTROLS	SEC566 Implementing and Auditing CIS Controls™ GCCC
Cyber Risk Officer	
TECHNOLOGY LEADERSHIP	LDR512 Security Leadership Essentials for Managers™ GSLC
RISK & COMPLIANCE	LDR519 Cybersecurity Risk Management and Compliance™
INCIDENT RESPONSE	LDR553 Cyber Incident Management™ GCIL

Development paths built for current and aspiring CISOs, organized into distinct paths that develop focused expertise in strategy and culture, operational excellence, and enterprise risk leadership.

CYBER RANGES

Practice for Focused Job Functions	
CYBER DEFENSE	Cyber Defense NetWars
DIGITAL FORENSICS & INCIDENT RESPONSE	DFIR NetWars DFIR NetWars Continuous
INDUSTRIAL CONTROL SYSTEMS	ICS NetWars
POWER GENERATION AND DISTRIBUTION	GRID NetWars

These interactive hands-on learning exercises cover specific job roles for in-depth practical application and assessment of cybersecurity subject matter to help advance your career in a specific field.

ADVANCED CYBER DEFENSE | HARDEN SPECIFIC DEFENSES

Topic-Focused	
TRAFFIC ANALYSIS	SEC503 Network Monitoring and Threat Detection In-Depth™ GCIA
SIEM	SEC555 Detection Engineering and SIEM Analytics™ GCDA
PYTHON CODING	SEC573 AI-Powered Security Automation: Building Tools with Python, LLMs, and MCP™ GPVC SEC673 Advanced Information Security Automation with Python™
DATA SCIENCE	SEC595 Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™ GMLE
Open-Source Intelligence	
OSINT	SEC587 Advanced Open-Source Intelligence (OSINT) Gathering & Analysis™ GSOA

SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

Penetration Testing, Network, Web, and Cloud	
ARTIFICIAL INTELLIGENCE	SEC535 Offensive AI – Attack Tools and Techniques™ GOAA SEC598 AI and Security Automation for Red, Blue, and Purple Teams™ GASAE
CLOUD	SEC588 Cloud Penetration Testing™ GCPN
ENTERPRISE	SEC580 Metasploit for Enterprise Penetration Testing™
EXPLOIT DEVELOPMENT	SEC760 Advanced Exploit Development for Penetration Testers™
MOBILE APPS	SEC575 iOS and Android Application Security Analysis and Penetration Testing™ GMOB
PURPLE TEAM	SEC599 Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses™ GDAT SEC699 Advanced Purple Teaming – Adversary Emulation & Detection Engineering™
RED TEAM	SEC665 Advanced Red Team Operations SEC670 Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™
WIRELESS & IoT	SEC556 IoT Penetration Testing™ SEC617 Wireless Penetration Testing and Ethical Hacking™ GAWN

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

Specialization	
CLOUD FORENSICS	FOR509 Enterprise Cloud Forensics & Incident Response™ GCFR
RANSOMWARE	FOR528 Ransomware and Cyber Extortion™
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 FOR589 Cybercrime Investigations™
Digital Forensics and Media Exploitation	
SMARTPHONES	FOR585 Smartphone Forensic Analysis In-Depth™ GASF
MAC FORENSICS	FOR518 Mac and iOS Forensic Analysis and Incident Response™ GIME
LINUX FORENSICS	FOR577 Linux Incident Response and Threat Hunting™ GLIR
ARTIFICIAL INTELLIGENCE	FOR563 Applied AI for Digital Forensics and Incident Response: Leveraging Local Large Language Models™

CLOUD SECURITY SPECIALIZATIONS

Specialization for Advanced Skills and Roles	
APPLICATION SECURITY	SEC522 Application Security: Securing Web Apps, APIs, and Microservices™ GWEB
AI APPLICATION SECURITY	SEC545 GenAI and LLM Application Security™
IDENTITY SECURITY	SEC559 Cloud and Hybrid Identity Security™
CLOUD PEN TEST	SEC588 Cloud Penetration Testing™ GCPN
CLOUD FORENSICS	FOR509 Enterprise Cloud Forensics and Incident Response™ GCFR
AI & CLOUD TRANSFORMATION	LDR520 Emerging Trends for Cyber Leaders: AI and Cloud™
Specialized cloud security expertise across AI systems, application defense, identity security, penetration testing, forensics, and leadership, equipping teams to monitor, detect, and defend cloud environments at scale.	

ROLE-BASED TRAINING FROM SANS WORKFORCE SECURITY & RISK

ICS Cybersecurity Awareness Training	
NERC CIP Compliance Training	
Help protect critical systems by reinforcing the behavior your engineers, system operators and others who interact with operational technology environments require to prevent, identify and respond to cyber incidents.	

LEADERSHIP SPECIALIZATION

Management Specialization	
AI & CLOUD TRANSFORMATION	LDR520 Emerging Trends for Cyber Leaders: AI and Cloud™
Prepare security leaders to guide cloud and AI transformation and anticipate post-quantum risk through strategic governance and decision making.	

ROLE-BASED TRAINING FROM SANS WORKFORCE SECURITY & RISK

Security Essentials for Business Leaders and Managers	
Leadership-focused modules enable managers to efficiently build and sustain a secure digital environment crucial for business operations.	