# 2023 (Aug–Nov)
# MEA Events Schedule

**SANS | GIAC CERTIFICATIONS**

Hybrid = In-Person and Live Online

| | | | GIAC CERTIFICATIONS With Remote Proctoring | **Riyadh Cyber Leaders** Riyadh, SA 20–24 Aug | **Doha September** Doha, QA 16–21 Sep | **Cyber Safari** Riyadh, SA 7–19 Oct | **Gulf Region** Dubai, AE 4–23 Nov |
|---|---|---|---|---|---|---|---|
| **CLOUD** | SEC488 | Cloud Security Essentials | GCLD | | SEC488 Hybrid | | |
| **DFIR** | FOR500 | Windows Forensic Analysis | GCFE | | | FOR500 Hybrid | |
| | FOR578 | Cyber Threat Intelligence | GCTI | | | FOR578 Hybrid | |
| | FOR508 | Advanced Incident Response, Threat Hunting, and Digital Forensics | GCFA | | | | FOR508 Hybrid |
| | FOR585 | Smartphone Forensic Analysis In-Depth | GASF | | | | FOR585 Hybrid |
| **CYBER DEFENSE** | SEC401 | Security Essentials: Network, Endpoint, and Cloud | GSEC | | | SEC401 Hybrid | SEC401 Hybrid |
| | SEC497 | Security Essentials: Network, Endpoint, and Cloud | GOSI | | | | SEC497 Hybrid |
| | SEC501 | Advanced Security Essentials – Enterprise Defender | GCED | | | | SEC501 Hybrid |
| | SEC503 | Intrusion Detection In-Depth | GCIA | | | SEC503 Hybrid | |
| | SEC511 | Continuous Monitoring and Security Operations | GMON | | | SEC511 Hybrid | SEC511 Hybrid |
| | SEC530 | Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise | GDSA | | | | SEC530 Hybrid |
| **ICS** | ICS410 | ICS/SCADA Security Essentials | GICSP | | | | ICS410 Hybrid |
| | ICS418 | ICS Security Essentials for Managers | | | | | ICS418 Hybrid |
| | ICS515 | ICS Visibility, Detection, and Response | GRID | | ICS515 Hybrid | | ICS515 Hybrid |
| | ICS612 | ICS Cybersecurity In-Depth | | | | | ICS612 Hybrid |
| **LEADERSHIP** | MGT414 | SANS Training Program for the CISSP Certification | GISP | | | MGT414 Hybrid | |
| | MGT512 | Security Leadership Essentials for Managers | GSLC | MGT512 Hybrid | | | MGT512 Hybrid |
| | MGT514 | Security Strategic Planning, Policy, and Leadership | GSTRT | MGT514 Hybrid | | | MGT514 Hybrid |
| | SEC566 | Implementing and Auditing Security Frameworks and Controls | GCCC | | | SEC566 Hybrid | |
| **OFFENSIVE OPS** | SEC504 | Hacker Tools, Techniques, and Incident Handling | GCIH | | | SEC504 Hybrid | SEC504 Hybrid |
| | SEC560 | Enterprise Penetration Testing | GPEN | | | | SEC560 Hybrid |
| | SEC588 | Cloud Penetration Testing | GCPN | | | SEC588 Hybrid | |

# SANS Training Roadmap
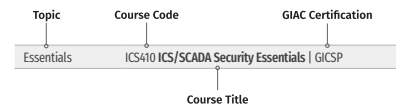
## Baseline Skills

### NEW TO CYBERSECURITY | COMPUTERS, TECHNOLOGY, AND SECURITY

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

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.

### CORE TECHNIQUES | PREVENT, DEFEND, MAINTAIN

Every Security Professional Should Know

| | |
|---|---|
| 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 **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.

### TECHNICAL TRAINING FROM SANS SECURITY AWARENESS

Security Essentials for IT Administrators

Protecting your organization from cyber threats requires continuous investment in skills development to stay ahead of any emerging threats. This short-form computer-based training provides technical teams with a deep understanding of evolving security concepts with a learning progression suited to their skillset.

### FORENSICS ESSENTIALS

Every Forensics and Incident Response Professional Should Know

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

### CLOUD SECURITY ESSENTIALS

Every Cloud Security Professional Should Know

| | |
|---|---|
| ESSENTIALS | 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. This course provides the basic knowledge required to introduce students to the cloud security industry, as well as in-depth, hands-on practice in labs.

### CLOUD FUNDAMENTALS

Built for professionals who need to be conversant in basic cloud security concepts, principles, and terms, but who are not responsible for hands-on cloud activities.

| | |
|---|---|
| INTRODUCTION | SEC388 **Intro to Cloud Computing and Security** |

### TECHNICAL TRAINING FROM SANS SECURITY AWARENESS

Developer Secure Code Training

Educate everyone involved in the software development process including developers, architects, managers, testers, business owners, and partners with role-focused training that ensures your team can properly build defensible applications from the start.

### 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** |

### FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know

| | |
|---|---|
| CISSP® TRAINING | LDR414 **SANS Training Program for CISSP® Certification** | GISP |
| SECURITY AWARENESS | LDR433 **Managing Human Risk** | SSAP |

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.

### CYBER RANGES

| | |
|---|---|
| CTF & TRIVIA | Bootup CTF |
| SKILLS ASSESSMENT & PRACTICAL APPLICATION | NetWars Core |

These cyber range offerings cover the broadest range of topics and are meant for all InfoSec professionals at all levels.

## 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: 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 | VULNERABILITY ANALYSIS, PENETRATION TESTING

Every Offensive Professional Should Know

| | |
|---|---|
| NETWORK PEN TESTING | SEC560 **Enterprise Penetration Testing** | 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 Incident Response Professional Should Know

| | |
|---|---|
| ENDPOINT FORENSICS | FOR500 **Windows Forensic Analysis** | GCFE |
| | FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA |
| | FOR532 **Enterprise Memory Forensics In-Depth** |
| | FOR577 **LINUX Incident Response & Analysis** |
| | 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.

### CORE CLOUD SECURITY

Preparation for More Focused Job Functions

| | |
|---|---|
| PUBLIC CLOUD | SEC510 **Public Cloud Security: AWS, Azure, and GCP** | GPCS |
| AUTOMATION & DEVSECOPS | SEC540 **Cloud Security and DevSecOps Automation** | GCSA |
| MONITORING & DETECTION | SEC541 **Cloud Security Attacker Techniques, Monitoring & Threat Detection** | GCTD |
| 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.

### 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 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 **Leading Cybersecurity Change: Building a Security-Based Culture** |

Operational Cybersecurity Executive

| | |
|---|---|
| VULNERABILITY MANAGEMENT | LDR516 **Building and Leading Vulnerability Management Programs** |
| SOC | LDR551 **Building and Leading Security Operations Centers** | GSOM |
| FRAMEWORKS & CONTROLS | SEC566 **Implementing and Auditing Security Frameworks & Controls** | GCCC |

### CYBER RANGES

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

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.

## 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 **Network Monitoring and Threat Detection In-Depth** | GCIA |
| SIEM | SEC555 **SIEM with Tactical Analytics** | GCDA |
| POWERSHELL | SEC586 **Security Automation with PowerShell** |
| PYTHON CODING | SEC573 **Automating Information Security with Python** | GPYC |
| | SEC673 **Advanced Information Security Automation with Python** |
| DATA SCIENCE | SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals** |

Open-Source Intelligence

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

### SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

Network, Web, and Cloud

| | |
|---|---|
| EXPLOIT DEVELOPMENT | SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN |
| | SEC661 **ARM Exploit Development** |
| | SEC760 **Advanced Exploit Development for Penetration Testers** |
| CLOUD PEN TEST | SEC588 **Cloud Penetration Testing** | GCPN |

Specialized Penetration Testing

| | |
|---|---|
| SOCIAL ENGINEERING | SEC467 **Social Engineering for Security Professionals** |
| BLOCKCHAIN | SEC554 **Blockchain and Smart Contract Security** |
| RED TEAM | SEC565 **Red Team Operations and Adversary Emulation** |
| | SEC670 **Red Teaming Tools - Developing Windows Implants, Shellcode, Command and Control** |
| MOBILE | SEC575 **iOS and Android Application Security Analysis and Penetration Testing** | GMOB |
| PRODUCT SECURITY | SEC568 **Combating Supply Chain Attacks with Product Security Testing** |
| PEN TEST | SEC580 **Metasploit for Enterprise Penetration Testing** |
| WIRELESS | SEC556 **IoT Penetration Testing** |
| | SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN |

Purple Team

| | |
|---|---|
| ADVERSARY EMULATION | SEC598 **Security Automation for Offense, Defense, and Cloud** |
| | 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 & Incident Response** | GCFR |
| RANSOMWARE | FOR528 **Ransomware for Incident Responders** |
| 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 Intelligence** |

Digital Forensics & 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 & Analysis** |

### SPECIALIZATION IN CLOUD SECURITY

Specialization for Advanced Skills & Roles

| | |
|---|---|
| APPLICATION SECURITY | SEC522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB |
| CLOUD PEN TEST | SEC588 **Cloud Penetration Testing** | GCPN |
| CLOUD FORENSICS | FOR509 **Enterprise Cloud Forensics and Incident Response** | GCFR |
| DESIGN & IMPLEMENTATION | MGT520 **Leading Cloud Security Design and Implementation** |

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

### TECHNICAL TRAINING FROM SANS SECURITY AWARENESS

ICS Engineer Training

Help protect critical systems by reinforcing the behavior your engineers, system operators and others who interact with ICS environments require to prevent, identify and respond to cyber incidents.

### LEADERSHIP SPECIALIZATIONS

Management Specialization

| | |
|---|---|
| AUDIT & MONITOR | AUD507 **Auditing Systems, Applications, and the Cloud** | GSNA |
| DESIGN & IMPLEMENTATION | LDR520 **Leading Cloud Security Design and Implementation** |
| LAW, DATA PRIVACY, & IP | LDR523 **Cybersecurity Law, Data Privacy, & Intellectual Property** |
| PROJECT MANAGEMENT | MGT525 **Managing Cybersecurity Initiatives & Effective Communication** | GCPM |
| INCIDENT RESPONSE | LDR553 **Cyber Incident Management** |

### MANAGE HUMAN RISK WITH TRAINING FROM SANS SECURITY AWARENESS

EndUser Awareness Training

Computer-based end-user training is built from a curated selection of the most pressing risk and compliance topics to address employee security behaviors. This engaging, modular, and multilingual suite of content reduces training fatigue and increases comprehension by tailoring your security awareness training program to the role- and industry-based issues relevant to your organization.