MENU

Cyber Defense Courses by Job Role

Join the Community

Full Course List

Our SANS Cyber Defense curriculum provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and applications against the most dangerous threats. Our courses are full of important and immediately useful techniques that you can put to work as soon as you return to your office. The curriculum has been developed through a consensus process involving industry leading engineers, architects, administrators, developers, security managers, and information security professionals.

Blue Teamer - All Around Defender

This job, which may have varying titles depending on the organization, is often characterized by the breadth of tasks and knowledge required. The all-around defender and Blue Teamer is the person who may be a primary security contact for a small organization, and must deal with engineering and architecture, incident triage and response, security tool administration and more.

SEC406: Essential Linux Skills for the Security Professional™

SEC450: Blue Team Fundamentals: Security Operations and Analysis™ (Certification: GSOC)

SEC503: Network Monitoring and Threat Detection In-Depth™ (Certification: GCIA)

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ (Certification: GMON)

SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™ (Certification: GDSA)

SEC555: Detection Engineering and SIEM Analytics™ (Certification: GCDA)

SEC573: Automating Information Security with Python™ (Certification: GPYC)

SEC673: Advanced Information Security Automation with Python™

LDR551: Building and Leading Security Operations Centers™

Security Architect & Engineer

Design, implement, and tune an effective combination of network-centric and data-centric controls to balance prevention, detection, and response. Security architects and engineers are capable of looking at an enterprise defense holistically and building security at every layer. They can balance business and technical requirements along with various security policies and procedures to implement defensible security architectures.

SEC406: Essential Linux Skills for the Security Professional™

SEC503: Network Monitoring and Threat Detection In-Depth™ (Certification: GCIA)

SEC511: Continuous Monitoring and Security Operations™ (Certification: GMON)

SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™ (Certification: GDSA)

Cybersecurity Analyst / Engineer

As this is one of the highest-paid jobs in the field, the skills required to master the responsibilities involved are advanced. You must be highly competent in threat detection, threat analysis, and threat protection. This is a vital role in preserving the security and integrity of an organization's data.

SEC401: Security Essentials: Network, Endpoint, and Cloud™ (Certification: GSEC)

SEC406: Essential Linux Skills for the Security Professional™

ICS410: ICS/SCADA Security Essentials™ (Certification: GICSP)

SEC450: Blue Team Fundamentals: Security Operations and Analysis™ (Certification: GSOC)

ICS456: Essentials for NERC Critical Infrastructure Protection™ (Certification: GCIP)

SEC501: Advanced Security Essentials - Enterprise Defender™ (Certification: GCED)

SEC503: Network Monitoring and Threat Detection In-Depth™ (Certification: GCIA)

SEC504: Hacker Tools, Techniques, and Incident Handling™ (Certification: GCIH)

FOR509: Enterprise Cloud Forensics and Incident Response™ (Certification: GCFR)

SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™ (Certification: GDSA)

SEC540: Cloud Native Security and DevSecOps Automation™ (Certification: GCSA)

SEC555: Detection Engineering and SIEM Analytics™ (Certification: GCDA)

SEC573: Automating Information Security with Python™

SEC673: Advanced Information Security Automation with Python™

OSINT Investigator/Analyst

These resourceful professionals gather requirements from their customers and then, using open sources and mostly resources on the internet, collect data relevant to their investigation. They may research domains and IP addresses, businesses, people, issues, financial transactions, and other targets in their work. Their goals are to gather, analyze, and report their objective findings to their clients so that the clients might gain insight on a topic or issue prior to acting.

SEC497: Practical Open-Source Intelligence (OSINT)™

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

FOR578: Cyber Threat Intelligence™ (Certification: GCTI)

Intrusion Detection / (SOC) Analyst

Security Operations Center (SOC) analysts work alongside security engineers and SOC managers to implement prevention, detection, monitoring, and active response. Working closely with incident response teams, a SOC analyst will address security issues when detected, quickly and effectively. With an eye for detail and anomalies, these analysts see things most others miss.

SEC406: Essential Linux Skills for the Security Professional™

SEC450: Blue Team Fundamentals: Security Operations and Analysis™ (Certification: GSOC)

SEC503: Network Monitoring and Threat Detection In-Depth™ (Certification: GCIA)

SEC504: Hacker Tools, Techniques, and Incident Handling™ (Certification: GCIH)

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics™ (Certification: GFCA)

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ (Certification: GMON)

SEC555: SIEM with Tactical Analytics™ (Certification: GCDA)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™ (Certification: GNFA)

SEC573: Automating Information Security with Python™

SEC673: Advanced Information Security Automation with Python™

SOC Manager

Security Operations Center (SOC) managers bridge the gap between business processes and the highly technical work that goes on in the SOC. They direct SOC operations and are responsible for hiring and training, creating and executing cybersecurity strategy, and leading the company's response to major security threats.

SEC406: Essential Linux Skills for the Security Professional™

SEC450: Blue Team Fundamentals: Security Operations and Analysis™ (Certification: GSOC)

SEC503: Network Monitoring and Threat Detection In-Depth™ (Certification: GCIA)

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ (Certification: GMON)

SEC504: Hacker Tools, Techniques, and Incident Handling™ (Certification: GCIH)

LDR551: Building and Leading Security Operations Centers™

SANS.edu Graduate Certificate in Cyber Defense Operations

Gain hands-on knowledge in the applied technologies and operational techniques needed to defend and secure information assets and business systems.

- Designed for working InfoSec and IT professionals
- Highly technical 12-credit-hour program
- Includes 4 industry-recognized GIAC certifications

Learn More

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email...

Select your country

By providing this information, you agree to the processing of your personal data by SANS as described in our Privacy Policy.

- ☐ SANS NewsBites
- ☐ @Risk: Security Alert
- ☐ OUCH! Security Awareness

Subscribe

Company

Mission

Instructors

About

FAQ

Press

Contact Us

Careers

Policies

Training Programs

Work Study

Academies & Scholarships

Public Sector Partnerships

Law Enforcement

SkillsFuture Singapore

Degree Programs

Get Involved

Join the Community

Become an Instructor

Become a Sponsor

Speak at a Summit

Join the CISO Network

Award Programs

Partner Portal