CompTIA Cyber Security Analyst (CSA+)

5 Days

Target Audience

CompTIA CSA+ certification is aimed at IT professionals with (or seeking) job roles such as IT Security Analyst, Security Operations Center (SOC) Analyst, Vulnerability Analyst, Cybersecurity Specialist, Threat Intelligence Analyst, and Security Engineer.

It is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers)
- Understand TCP/IP addressing, core protocols, and troubleshooting tools
- Identify network attack strategies and defenses
- Know the technologies and uses of cryptographic standards and products
- Identify network- and host-based security technologies and practices
- Describe the standards and products used to enforce security on web and communications technologies

Course Outline

Module 1 / Threat Management (1)

- **Cybersecurity Analysts** • Cybersecurity Roles and Responsibilities • Frameworks and Security Controls • Risk Evaluation • Penetration Testing Processes
- **Reconnaissance Techniques** • The Kill Chain • Open Source Intelligence • Social Engineering • Topology Discovery • Service Discovery • OS Fingerprinting • Labs • OSINT • VM Orientation • Host, Topology, and Service Discovery with Nmap

Module 2 / Vulnerability Management

- **Managing Vulnerabilities** • Vulnerability Management Requirements • Asset Inventory • Data Classification • Vulnerability Management Processes • Vulnerability Scanners • Microsoft Baseline Security Analyzer • Vulnerability Feeds and SCAP • Configuring Vulnerability Scans • Vulnerability Scanning Criteria • Exploit Frameworks • Labs • Vulnerability Scanning with OpenVAS and MBSA
- **Remediating Vulnerabilities** • Analyzing Vulnerability Scans • Remediation and Change Control • Remediating Host Vulnerabilities • Remediating Network Vulnerabilities • Remediating Virtual Infrastructure Vulnerabilities
- **Secure Software Development** • Software Development Lifecycle • Software Vulnerabilities • Software Security Testing • Interception Proxies • Web Application Firewalls • Source Authenticity • Reverse Engineering • Labs • Web Application Testing with Nikto and Burpsuite

Module 3 / Threat Management (2)

- **Security Appliances** • Configuring Firewalls • Intrusion Detection and Prevention • Configuring IDS • Malware Threats • Configuring Anti-virus Software • Sysinternals • Enhanced Mitigation Experience Toolkit • Labs • Network Security Monitoring with Snort and Security Onion • Malware Analysis with Sysinternals
- **Logging and Analysis** • Packet Capture • Packet Capture Tools • Monitoring Tools • Log Review and SIEM • SIEM Data Outputs • SIEM Data Analysis • Point-in-Time Data Analysis • Labs • Packet Analysis with Wireshark and Network Miner • SIEM with OSSIM

Module 4 / Cyber Incident Response

- **Incident Response** • Incident Response Processes • Threat Classification • Incident Severity and Prioritization • Types of Data
- **Forensics Tools** • Digital Forensics Investigations • Documentation and Forms • Digital Forensics Crime Scenes • Digital Forensics Kits • Image Acquisition • Password Cracking • Analysis Utilities • Labs • Forensic Image Analysis with Autopsy
- **Incident Analysis and Recovery** • Analysis and Recovery Frameworks • Analyzing Network Symptoms • Analyzing Host Symptoms • Analyzing Data Exfiltration • Analyzing Application Symptoms • Using Sysinternals • Containment Techniques • Eradication Techniques • Validation Techniques • Corrective Actions • Labs • Red Team Versus Blue Team

Module 5 / Security Architecture

- **Secure Network Design** • Network Segmentation • Blackholes, Sinkholes, and Honeypots • System Hardening • Group Policies and MAC • Endpoint Security • Labs • Network Segmentation with pfSense
- **Managing Identities and Access** • Network Access Control • Identity Management • Identity Security Issues • Identity Repositories • Context-based Authentication • Single Sign On and Federation • Exploiting Identities • Exploiting Web Browsers and Applications • Labs • Secure Appliance Administration • Email Spoofing and XSS
- **Security Frameworks and Policies** • Frameworks and Compliance • Reviewing Security Architecture • Procedures and Compensating Controls • Verifications and Quality Control • Security Policies and Procedures • Personnel Policies and Training