COMPTIA CSA+ CYBERSECURITY ANALYST CS001

Ctrl+ Click here to enquire

Course Duration: 5 days

Course description

Overview:

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. As attackers have learned to evade traditional signature-based solutions such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by CSA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface.

Course Objectives

After completing this course, students will be able to:

- Configure and use threat detection tools.
- Perform data analysis.
- Interpret the results to identify vulnerabilities, threats and risks to an organization.

Prerequisites

Before attending this course, students must have:

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

COMPTIA CSA+ CYBERSECURITY ANALYST CS001

Ctrl+ Click here to enquire

Course Content

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

Module 2 – Threat Management 2

- **Security Appliances** • Configuring Firewalls • Intrusion Detection and Prevention • Configuring IDS • Malware Threats • Configuring Anti-virus Software • Sysinternals • Enhanced Mitigation Experience Toolkit
- **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

Module 3 – 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
- **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

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 Scene • Digital Forensics Kits • Image Acquisition • Password Cracking • Analysis Utilities**
- **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**

Module 5 – Security Architecture

- **Secure Network Design • Network Segmentation • Blackholes, Sinkholes, and Honeypots • System Hardening • Group Policies and MAC • Endpoint Security**
- **Managing Identities and Access • Network Access Control • Identity Management • Identity Security Issues • Identity Repositories • Context-based Authentication • Single Sign On and Federations • Exploiting Identities • Exploiting Web Browsers and Applications**
- **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**