CompTIA Cybersecurity Analyst (CompTIA CYSA+)

Modality: Virtual Classroom

Duration: 5 Days

About this Course:

As attackers have learned to evade traditional signature-based solutions, such as firewalls and anti-virus software, an analytics-based approach within the IT security industry is increasingly important for organizations. CompTIA CySA+ applies behavioral analytics to networks to improve the overall state of security through identifying and combating malware and advanced persistent threats (APTs), resulting in an enhanced threat visibility across a broad attack surface. It will validate an IT professional's ability to proactively defend and continuously improve the security of an organization. CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

Course Objectives:

- Assess and respond to security threats and operate a systems and network security analysis platform.
- Assess information security risk in computing and network environments.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.
- Address security issues with the organization's technology architecture.

Prerequisites:

While there is no required prerequisite, the CompTIA CySA+ certification is intended to follow CompTIA Security+ or equivalent experience. It is recommended for CompTIA CySA+ certification

candidates to have the following:

- 3-4 years of hands-on information security or related experience
- Network+, Security+, or equivalent knowledge

Course Outline:

COURSE OUTLINE

- Lesson 1: Explaining the Importance of Security Controls and Security Intelligence
- Lesson 2: Utilizing Threat Data and Intelligence
- Lesson 3: Analyzing Security Monitoring Data
- Lesson 4: Collecting and Querying Security Monitoring Data
- Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques
- Lesson 6: Applying Incident Response Procedures
- Lesson 7: Applying Risk Mitigation and Security Frameworks
- Lesson 8: Performing Vulnerability Management
- Lesson 9: Applying Security Solutions for Infrastructure Management
- Lesson 10: Understanding Data Privacy and Protection
- Lesson 11: Applying Security Solutions for Software Assurance
- Lesson 12: Applying Security Solutions for Cloud and Automation

LABS OUTLINE

- Analyzing Output from Network Security Monitoring Tools
- Discovering the Lab Environment
- Analyzing Output from Security Appliance Logs
- Analyzing Output from Endpoint Security Monitoring Tools
- Analyzing Email Headers
- Configuring SIEM Agents and Collectors
- Analyzing, Filtering, and Searching Event Log and syslog Output
- Collecting and Validating Digital Evidence
- Analyzing Network-related IoCs
- Analyzing Host and Application IoCs
- Observing IoCs during a Security Incident
- Analyzing Output from Topology and Host Enumeration Tools
- Testing Credential Security
- Configuring Vulnerability Scanning and Analyzing Outputs
- Assessing Vulnerability Scan Outputs
- Assessing the Impact of Regulation on Vulnerability Management
- Performing Account and Permissions Audits
- Configuring Network Segmentation and Security
- Configuring and Analyzing Share Permissions
- Assessing the Impact of Web Application Vulnerabilities
- Analyzing Output from Web Application Assessment Tools
- Analyzing Output from Cloud Infrastructure Assessment Tools