CompTIA Cybersecurity Analyst (CS0-004)

Course Overview

CompTIA Cybersecurity Analyst (CySA+) is an intermediate-level, vendor-neutral cybersecurity certification that validates the knowledge and skills required to detect, analyze, and respond to cybersecurity threats and vulnerabilities in a Security Operations Center (SOC) or vulnerability management environment.

Course Objectives

By the end of this CompTIA CySA+ course, students will be able to:

- Explain SOC foundations by mastering cybersecurity concepts, governance, policies, and incident response basics.
- Apply risk strategies and threat modeling frameworks to mitigate organizational risks.
- Manage and harden systems to reduce attack surfaces through robust configuration management.
- Analyze system architectures across traditional networks, modern infrastructure, and critical industrial controls.
- Implement access management by securing identities, endpoints, devices, and applying cryptography for data protection.
- Leverage threat intelligence and actor concepts to conduct proactive threat hunting operations.
- Assess network vulnerabilities using specialized tools to scan, analyze, prioritize, and report findings.
- Manage incident response communications by tracking logs, handling escalations, and monitoring key metrics.
- Execute incident response plans using established attack methodology frameworks and specialized containment techniques.
- Analyze malicious activity by identifying host, network, and application indicators of compromise (IoCs).
- Automate data analysis through scripting fundamentals, security analytics, and pattern recognition.
- Optimize security operations by integrating tools, standardizing workflows, and managing AI risks and capabilities.
- Assess application vulnerabilities within both traditional web environments and cloud infrastructures.
- Secure application software by implementing secure development practices and mitigating application-layer attacks.

Target Student

The certification is designed for professionals with 4 years of hands-on experience in a SOC analyst (Level2) or vulnerability analyst role.

Course Prerequisites

To ensure your success in this course, you should have four years of hands-on experience as an incident response analyst or security operations center (SOC) analyst. CompTIA Network+, Security+, or the equivalent knowledge is strongly recommended.

Associated Certifications

Cybersecurity Analyst (CySA+)

Table of Contents

10.0 Analyzing Malicious Activity
- 10.1 Threat Detection and Analysis Tools
- 10.2 Host Indicators of Compromise
- 10.3 Network Indicators of Compromise
- 10.4 Application and Web-based Indicators

11.0 Automating Data Analysis
- 11.1 Scripting Fundamentals
- 11.2 Scripting Languages
- 11.3 Security Analytics and Pattern Recognition
- 11.4 Technology and Tool Integration

12.0 Improving Processes with Automation
- 12.1 Standardization and Team Coordination
- 12.2 Automation, Orchestration, and Enrichment
- 12.3 AI Risks and Governance
- 12.4 AI in Security Operations

13.0 Assessing Application Vulnerabilities
- 13.1 Web and Application Vulnerability Analysis
- 13.2 Cloud Vulnerability Assessment

14.0 Securing Applications
- 14.1 Secure Software Development and Testing
- 14.2 Application Attack Identification and Mitigation