

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

1.0 Identifying Security Operations Fundamentals

1.1 Cybersecurity Foundations

1.2 Governance, Policies, and Controls

1.3 Introduction to Incident Response in the SOC

2.0 Applying Risk Management Strategies

2.1 Risk Concepts

2.2 Threat Modeling Frameworks

3.0 Managing System Security and Configurations

3.1 Attack Surface Management

3.2 System Hardening

4.0 Comparing System Architectures

4.1 Infrastructure and System Architecture

4.2 Modern Network Architectures

4.3 Critical Infrastructure and Industrial Controls

5.0 Applying Access Management

5.1 Identity and Access Management

5.2 Device and Endpoint Management

5.3 Data Protection and Cryptography

6.0 Threat Intelligence and Threat Hunting

6.1 Threat Actor Concepts

6.2 Threat Intelligence Sources

6.3 Threat Hunting

7.0 Assessing Network Vulnerabilities

7.1 Vulnerability Scanning Foundations

7.2 Vulnerability Scan Types

7.3 Select Vulnerability Tools

7.4 Vulnerability Analysis and Prioritization

7.5 Vulnerability and Incident Reporting

8.0 Managing Incident Response and Communication

8.1 Manage Logs

8.2 Incident Escalation

8.4 Incident Response Metrics

9.0 Executing Incident Response Plans

9.1 Attack Methodology Frameworks

9.2 The Incident Response Process

9.3 Incident Response Techniques

- 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

For More Information Please Contact: Vnohow (Thailand) Co., Ltd.

90/31 Sathorn Thani Building 1, 12FL, North Sathorn Road, Silom, Bangrak, Bangkok 10500 Thailand
Tel +662-634-3287-9, +662-634-3299 Email vnohow@vnohow.com Website www.vnohow.com