Document Generated: 11/28/2026

Learning Style: On Demand

Technology: CompTIA

Difficulty: Intermediate

Course Duration: 1 Week

CompTIA CySA+



The CompTIA CySA+ (Cybersecurity Analyst) course prepares IT and cybersecurity professionals to proactively detect, analyse, and respond to cyber threats using behavioural analytics and industry best practices. Unlike certifications that focus primarily on implementing security controls, CySA+ emphasises continuous security monitoring, vulnerability management, threat hunting, incident response, and security operations within modern enterprise environments. Through hands-on exercises and real-world scenarios, learners will develop the skills to identify indicators of compromise, assess and prioritise vulnerabilities, investigate security

events, analyse logs, and recommend effective remediation strategies.

Course Objectives:

- Detect and analyse indicators of malicious activity.
- Apply threat hunting and threat intelligence concepts to identify emerging threats.
- Use appropriate tools and techniques to manage, prioritise, and respond to vulnerabilities and cyberattacks.
- Perform incident response activities, including investigation, containment, eradication, and recovery.
- Analyse security events and log data from multiple sources to identify suspicious behaviour.
- Implement and recommend security controls to improve an organisation's security posture.
- Communicate findings and create reports related to vulnerability management and incident response

Audience:

- Cybersecurity Analysts
- SOC (Security Operations Center) Analysts
- Threat Intelligence Analysts
- Vulnerability Analysts
- Incident Response Analysts
- Security Engineers

Prerequisites

There are no mandatory prerequisites for taking the CompTIA CySA+ certification exam. However, CompTIA recommends that candidates have:

- CompTIA Network+ and Security+ certifications, or equivalent knowledge.
- Approximately 3–4 years of hands-on experience in information security or a related IT security role.

Course Outline:

- **Module 1: Understanding Vulnerability Response, Handling, and Management**
    - Topic 1A: Understanding Cybersecurity Leadership Concepts
    - Topic 1B: Exploring Control Types and Methods
    - Topic 1C: Explaining Patch Management Concepts
- **Module 2: Exploring Threat Intelligence and Threat Hunting Concepts**
    - Topic 2A: Exploring Threat Actor Concepts
    - Topic 2B: Identifying Active Threats
    - Topic 2C: Exploring Threat-Hunting Concepts
- **Module 3: Explaining Important System and Network Architecture Concepts**
    - Topic 3A: Reviewing System and Network Architecture Concepts
    - Topic 3B: Exploring Identity and Access Management (IAM)
    - Topic 3C: Maintaining Operational Visibility
- **Module 4: Understanding Process Improvement in Security Operations**
    - Topic 4A: Exploring Leadership in Security Operations
    - Topic 4B: Understanding Technology for Security Operations
- **Module 5: Implementing Vulnerability Scanning Methods**
    - Topic 5A: Explaining Compliance Requirements
    - Topic 5B: Understanding Vulnerability Scanning Methods
    - Topic 5C: Exploring Special Considerations in Vulnerability Scanning
- **Module 6: Performing Vulnerability Analysis**
    - Topic 6A: Understanding Vulnerability Scoring Concepts
    - Topic 6B: Exploring Vulnerability Context Considerations
- **Module 7: Communicating Vulnerability Information**
    - Topic 7A: Explaining Effective Communication Concepts
    - Topic 7B: Understanding Vulnerability Reporting Outcomes and Action Plans
- **Module 8: Explaining Incident Response Activities**
    - Topic 8A: Exploring Incident Response Planning
    - Topic 8B: Performing Incident Response Activities
- **Module 9: Demonstrating Incident Response Communication**
    - Topic 9A: Understanding Incident Response Communication
    - Topic 9B: Analyzing Incident Response Activities
- **Module 10: Applying Tools to Identify Malicious Activity**
    - Topic 10A: Identifying Malicious Activity
    - Topic 10B: Explaining Attack Methodology Frameworks
    - Topic 10C: Explaining Techniques for Identifying Malicious Activity
- **Module 11: Analyzing Potentially Malicious Activity**
    - Topic 11A: Exploring Network Attack Indicators
    - Topic 11B: Exploring Host Attack Indicators
    - Topic 11C: Exploring Vulnerability Assessment Tools
- **Module 12: Understanding Application Vulnerability Assessment**
    - Topic 12A: Analyzing Web Vulnerabilities
    - Topic 12B: Analyzing Cloud Vulnerabilities

- **Module 13: Exploring Scripting Tools and Analysis Concepts**
    - Topic 13A: Understanding Scripting Languages
    - Topic 13B: Identifying Malicious Activity Through Analysis
- **Module 14: Understanding Application Security and Attack Mitigation Best Practices**
    - Topic 14A: Exploring Secure Software Development Practices
    - Topic 14B: Recommending Controls to Mitigate Successful Application Attacks
    - Topic 14C: Implementing Controls to Prevent Attacks