800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

CompTIA CySA+ Training

CompTIA Authorized Training · Applied Technology Academy

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.

LEVEL	DURATION	EXAM	EXPERIENCE	AVERAGE SALARY
Intermediate	**5 Days**	**CS0-004**	**4 years: SOC/vulnerability analysis**	**$112,000**

Course Overview

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to detect and analyze indicators of malicious activity, understand threat intelligence and threat management, respond to attacks and vulnerabilities, perform incident response, and report and communicate related activity.

Acquired Skills

Security Operations - Improve processes in security operations and differentiate between threat intelligence and threat hunting concepts as well as identify and analyze malicious activity using the appropriate tools and techniques.

Vulnerability Management - Implement and analyze vulnerability assessments, prioritize vulnerabilities, and make recommendations on mitigating attacks and vulnerability response.

Incident Response and Management - Apply updated concepts of attack methodology frameworks, perform incident response activities, and understand the incident management lifecycle.

Reporting and Communication - Apply communication best practices in vulnerability management and incident response as it relates to stakeholders, action plans, escalation, and metrics.

Course Outline

- **Lesson 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
- **Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts**
  - Topic 2A: Exploring Threat Actor Concepts
  - Topic 2B: Identifying Active Threats

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Topic 2C: Exploring Threat-Hunting Concepts
- **Lesson 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
- **Lesson 4: Understanding Process Improvement in Security Operations**
  - Topic 4A: Exploring Leadership in Security Operations
  - Topic 4B: Understanding Technology for Security Operations
- **Lesson 5: Implementing Vulnerability Scanning Methods**
  - Topic 5A: Explaining Compliance Requirements
  - Topic 5B: Understanding Vulnerability Scanning Methods
  - Topic 5C: Exploring Special Considerations in Vulnerability Scanning
- **Lesson 6: Performing Vulnerability Analysis**
  - Topic 6A: Understanding Vulnerability Scoring Concepts
  - Topic 6B: Exploring Vulnerability Context Considerations
- **Lesson 7: Communicating Vulnerability Information**
  - Topic 7A: Explaining Effective Communication Concepts
  - Topic 7B: Understanding Vulnerability Reporting Outcomes and Action Plans
- **Lesson 8: Explaining Incident Response Activities**
  - Topic 8A: Exploring Incident Response Planning
  - Topic 8B: Performing Incident Response Activities
- **Lesson 9: Demonstrating Incident Response Communication**
  - Topic 9A: Understanding Incident Response Communication
  - Topic 9B: Analyzing Incident Response Activities
- **Lesson 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
- **Lesson 11: Analyzing Potentially Malicious Activity**
  - Topic 11A: Exploring Network Attack Indicators
  - Topic 11B: Exploring Host Attack Indicators
  - Topic 11C: Exploring Vulnerability Assessment Tools
- **Lesson 12: Understanding Application Vulnerability Assessment**
  - Topic 12A: Analyzing Web Vulnerabilities
  - Topic 12B: Analyzing Cloud Vulnerabilities
- **Lesson 13: Exploring Scripting Tools and Analysis Concepts**

  - Topic 13A: Understanding Scripting Languages
  - Topic 13B: Identifying Malicious Activity Through Analysis
- **Lesson 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

Intended Audience

- Primary Job Roles
- Security Analyst
- Security Operations Center (SOC) Analyst
- Secondary Job Roles
- Vulnerability Management Analyst
- Security Engineer
- Threat Hunter

Prerequisites

Minimum of 4 years of hands-on experience as an incident response analyst or security operations center (SOC) analyst or equivalent experience.

Follow-On Courses

- CompTIA SecurityX
- CompTIA PenTest+
- Systems Security Certified Practitioner (SSCP)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.