CompTIA CySA+ Training Course

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring.

SEC-201

Course Outcomes

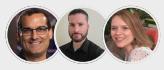
Professional, practical, & hands-on live instructor-led training

Further your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

Start Today

Potential Career Tracks

Incident Response Analyst · Vulnerability Analyst · Cybersecurity Engineer · Cybersecurity Analyst · Vulnerability Analyst · Application Security Analyst



Taught by Industry Veterans & World Class Instructors

Introduction to CompTIA CySA+

Course Overview

Intellectual Point's comprehensive CompTIA CySA+ training program is designed to provide you with the skills and knowledge necessary to excel in cybersecurity analytics and prepare for the CompTIA CySA+ certification exam. This course offers a deep dive into the methods and techniques used by cybersecurity professionals to detect, analyze, and respond to security threats and vulnerabilities. It is structured to not only make you proficient in key concepts but also thoroughly prepare you to pass the exam and succeed in real-world cybersecurity roles.

Throughout the course, you will gain hands-on experience with threat detection, incident response, vulnerability management, and security operations. The training emphasizes practical skills and problem-solving techniques that can be applied in everyday security tasks. Whether you're just starting your career in cybersecurity or you are looking to validate and strengthen your skills, this course equips you with the knowledge and confidence to secure your organization's assets and data against emerging threats.

Obtainable Skills

Threats and vulnerabilities · Identity and access management · Forensics · Security architecture · Cryptography and PKI · Risk management · Enterprise networks · Hybrid/cloud operations · Incident response

Course Insights

Audience Profile

This course is designed for IT professionals, network administrators, and individuals seeking to build a career in cybersecurity. It is ideal for those preparing for the CompTIA Security+ certification exam, as well as those looking to deepen their knowledge of network security, threat management, and risk mitigation.

Whether you're an entry-level professional, someone transitioning into cybersecurity, or an experienced IT professional looking to expand your skill set, this training provides a solid foundation in security principles. The course is beginner-friendly, making it accessible for those with no prior cybersecurity experience.

Course Outcomes

By the end of this course, participants will:

1. Master systematic approaches for scanning, analyzing, and patching system flaws.
2. Acquire skills to research, detect, and neutralize active threats with proactive measures.
3. Explore advanced techniques to harden systems, manage access, and maintain visibility.
4. Discover leadership principles, automate tasks, and refine processes for continuous improvement.
5. Identify, exploit, and mitigate vulnerabilities in web, cloud, and software to protect critical assets.

Module by Module Learning *Outline*

4 Modules

Module 1: Security Operations

Learning Objectives:

- Understand the key concepts of system and network architecture in security operations.
- Analyze indicators of potentially malicious activities using appropriate tools and techniques.

Topics Covered

System and Network Architecture in Security:

- Importance of system architecture in security operations.
- Concepts of network architecture, identity and access management, encryption, and sensitive data protection.

Analyzing Malicious Activity:

- Indicators of network-related, host-related, and application-related malicious activities.
- Tools and techniques for determining malicious activities.

Module 2: Vulnerability Management

Learning Objectives:

- Implement effective vulnerability scanning methods and analyze assessment outputs.
- Prioritize vulnerabilities using analysis data and recommend mitigation controls.

Topics Covered

Vulnerability Scanning and Analysis:

- Methods for asset discovery and scanning (internal vs. external, agent vs. agentless).
- Analyzing output from vulnerability assessment tools.

Prioritizing Vulnerabilities:

- Interpreting the Common Vulnerability Scoring System (CVSS).
- Factors affecting prioritization: exploitability, asset value, zero-day vulnerabilities.

Module 3: Incident Response & Management

Learning Objectives:

- Explain attack methodology frameworks relevant to cybersecurity incident response.
- Perform critical incident response activities and understand incident lifecycle phases.

Topics Covered

Attack Methodology Frameworks:

- Overview of frameworks such as Cyber kill chains and MITRE ATT&CK.
- Introduction to the Diamond Model of Intrusion Analysis.

Performing Incident Response:

- Processes involved in detection, analysis, containment, eradication, and recovery.
- Preparation and post-incident activities in incident management.

Module 4: Reporting & Communication

Learning Objectives:

- Understand the role of effective reporting and communication in vulnerability management.
- Highlight the importance of incident response reporting and the communication process.

Topics Covered

Vulnerability Management Reporting:

- Types of reports: compliance, action plans, and vulnerability management.
- Communicating key metrics and KPIs to stakeholders.

Incident Response Reporting and Communication:

- Steps in incident declaration and escalation.
- Conducting root cause analysis and reporting findings.