Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CySA+ - Cybersecurity Analyst

Course Description & Overview

SecureNinja's CompTIA Cybersecurity Analyst (CySA+) certification training is designed to validate the expertise of IT professionals in detecting, analyzing, and responding to cybersecurity threats and incidents. It emphasizes threat detection, vulnerability management, incident response, and security monitoring in enterprise environments.

CySA+ focuses on proactive security operations through techniques such as threat intelligence, behavioral analytics, security automation, and advanced network monitoring. The course provides hands-on experience using industry-standard tools and methodologies to identify and mitigate cyber threats.

Why Choose CompTIA CySA+

CompTIA CySA+ is a recognized industry certification that validates intermediate-level security skills essential for cybersecurity analysts. It emphasizes threat detection and response, equipping professionals with advanced security analytics, incident response techniques, and threat intelligence integration. Designed with a Security Operations Center (SOC) focus, it is ideal for SOC analysts, incident responders, and security professionals seeking to enhance their threat monitoring capabilities. As a vendor-neutral certification, CySA+ provides expertise applicable to multiple security tools and enterprise environments, ensuring professionals can adapt to different security infrastructures. The certification also emphasizes performance-based learning, incorporating real-world simulations and hands-on exercises to reinforce threat analysis and response skills, preparing candidates for practical cybersecurity challenges.

Topics Covered

- Security Operations – Security monitoring, threat hunting, and network traffic analysis
- Vulnerability Management – Conducting vulnerability assessments, risk prioritization, and remediation strategies
- Incident Response – Investigating security incidents, digital forensics, and crisis management
- Reporting & Communication – Analyzing security data, compliance reporting, and stakeholder communication
- Threat Intelligence – Implementing proactive defense strategies and using threat intelligence feeds
- Security Automation – Using SIEM, SOAR, and machine learning for security event correlation and response

Who is it for

- Security Analysts – Monitoring network traffic, detecting anomalies, and responding to threats
- Incident Response Teams – Investigating security incidents, analyzing malicious activity, and performing forensic analysis

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- SOC Analysts – Managing and defending against cyberattacks in a Security Operations Center environment
- Threat Hunters – Identifying unknown cyber threats through behavioral analysis and intelligence research
- IT Professionals – Expanding their cybersecurity skillset in threat management, monitoring, and response

Who Would Benefit

- IT professionals transitioning into cybersecurity analysis or incident response
- Security specialists aiming to enhance their threat detection and response capabilities
- Organizations seeking skilled professionals to secure enterprise environments against evolving threats

Prerequisites

- No formal prerequisites, but CompTIA Security+ or equivalent experience is recommended
- Recommended Experience: Four years of hands-on security experience as an incident response analyst or SOC analyst
- Understanding of networking, security frameworks, and risk management is beneficial

Course Outline

Module 1: Security Operations

- Analyzing network and system logs to detect malicious activity
- Implementing security monitoring strategies and threat detection techniques
- Understanding threat intelligence sources and attack methodologies

Module 2: Vulnerability Management

- Conducting vulnerability assessments and prioritizing security risks
- Using industry tools such as Nessus, OpenVAS, and Metasploit for security analysis
- Applying security controls to mitigate known vulnerabilities

Module 3: Incident Response and Management

- Identifying indicators of compromise (IoCs) and responding to cybersecurity incidents
- Digital forensics and evidence collection techniques
- Implementing incident response frameworks such as NIST and MITRE ATT&CK

Module 4: Reporting and Communication

- Developing security reports and compliance documentation
- Communicating security findings to stakeholders and leadership teams
- Creating action plans for security improvements and risk mitigation

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Course Length

- 5 Days
- 40 Hours

Exam Details

- Exam Number CS0-003
- Number of Questions: Up to 85
- Question Types: Multiple-choice & performance-based
- Duration: 165 minutes
- Passing Score: 750 (on a scale of 100-900)

The CompTIA CySA+ (CS0-003) certification prepares IT professionals for proactive threat detection, incident response, and vulnerability management in enterprise environments. With a strong emphasis on real-world security operations and analytics, this course provides hands-on training to identify, assess, and mitigate cybersecurity threats effectively.