CompTIA Cybersecurity Analyst CYSA+

Duration: 5 days
Audience: Professionnel TI

Who is this training for?

- IT Security Analyst
- Security Operations Center Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer, Cybersecurity Analyst
- Security Architect

Training objectives

- Explain the importance of threat data and intelligence
- Use threat intelligence to support the organization's security
- Perform vulnerability management activities
- Analyze the output of common vulnerability assessment tools
- Explain threats and vulnerabilities associated with specialized technology
- Explain threats and vulnerabilities associated with cloud exploitation
- Implement controls to Mitigate attacks and software vulnerabilities
- Apply security solutions for infrastructure management
- Explain software assurance best practices
- Explain hardware assurance best practices
- Analyze data as part of security monitoring activities
- Implement configuration changes to existing controls to improve security
- Explain the importance of proactive threat hunting
- Compare and contrast automation concepts and technologies
- Explain the importance of the incident response process

- Apply the appropriate incident response procedure
- Analyze potential indicators of compromise
- Use basic digital forensics techniques
- Understand the importance of privacy and data protection
- Apply security concepts in support of organizational risk mitigation
- Explain the importance of frameworks, policies, procedures and controls

Summary

CySA+ focuses on the ability to not only capture, monitor, and proactively respond to network traffic outcomes, but also emphasizes software and application security, automation, threat hunting, and compliance with IT regulations, which affects the daily work of security analysts. CySA+ covers the most up-to-date skills of security analysts and the professional skills used by threat intelligence analysts, application security analysts, compliance analysts, incident responders and managers, and threat hunters, bringing new techniques to combat threats inside and outside the Security Operations Center (SOC).

Course outline

- Explaining the Importance of Security Controls and Security Intelligence
- Utilizing Threat Data and Intelligence
- Analyzing Security Monitoring Data
- Collecting and Querying Security Monitoring Data
- Utilizing Digital Forensics and Indicator Analysis Techniques
- Applying Incident Response Procedures
- Applying Risk Mitigation and Security Frameworks
- Performing Vulnerability Management
- Applying Security Solutions for Infrastructure Management
- Understanding Data Privacy and Protection
- Applying Security Solutions for Software Assurance
-

Applying Security Solutions for Cloud and Automation

Approach and methodology

Analytical, data-driven approach, with a focus on behavioral analysis, threat hunting, automation, and incident response from real-world cybersecurity cases.

Recommendations

- Network+ or equivalent content, Security+ or equivalent content.
- Minimum of 4 years of practical experience in information security or related experience.

Certifications

Related Exam: CompTIA CySA+ (CS0-003) (or current version) Certification Earned: CompTIA Cybersecurity Analyst (CySA+) ® Course Link: Prepares for the CySA+ exam, with a focus on threat analysis, detection, and response.

Legal notices