CompTIA Cybersecurity Analyst+ CertPrep (CySA+)

CompTIA

- **Nível:** Avançado
- **Duração:** 35h

Sobre o curso

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.

As attackers have learned to evade traditional signature-based solutions, such as firewalls and anti-virus software, an analytics-based approach within the IT security industry is increasingly important for organizations.

CompTIA CySA+ applies behavioral analytics to networks to improve the overall state of security through identifying and combating malware and advanced persistent threats (APTs), resulting in an enhanced threat visibility across a broad attack surface. It will validate an IT professional's ability to proactively defend and continuously improve the security of an organization.

In this course you will gain the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

In addition, this course prepares you to pass the CompTIA CySA+ exam and earn the corresponding certification.

CompTIA CySA+ Certification

- CompTIA CySA+ is the only intermediate high-stakes cybersecurity analyst certification with both hands-on, performance-based questions and multiple-choice questions.

- CySA+ focuses on the candidates ability to not only proactively capture, monitor, and respond to network traffic findings, but also emphasizes software and application security, automation, threat hunting, and IT regulatory compliance, which affects the daily work of security analysts.
- CySA+ covers the most up-to-date core security analyst skills and upcoming job skills used by threat intelligence analysts, application security analysts, compliance analysts, incident responders/handlers, and threat hunters, bringing new techniques for combating threats inside and outside of the Security Operations Center (SOC)

Destinatários

The CompTIA CySA+ certification is designed for:

- IT security analysts,
- Threat intelligence analysts
- Security engineers
- Application security analysts
- Incident response or handlers
- Compliance analysts
- Threat hunters

Pré-requisitos

Recommended:

- Network+, Security+ or equivalent knowledge.
- Minimum of 4 years of hands-on information security or related experience.

Programa

- Understanding Vulnerability Response, Handling, and Management
- Exploring Threat Intelligence and Threat Hunting Concepts
- Explaining Important System and Network Architecture Concepts
- Understanding Process Improvement in Security Operations
- Implementing Vulnerability Scanning Methods
- Performing Vulnerability Analysis
- Communicating Vulnerability Information
- Explaining Incident Response Activities

- Demonstrating Incident Response Communication
- Applying Tools to Identify Malicious Activity
- Analyzing Potentially Malicious Activity
- Understanding Application Vulnerability Assessment
- Exploring Scripting Tools and Analysis Concepts
- Understanding Application Security and Attack Mitigation Best Practices

Understanding Vulnerability Response, Handling, and Management

- Understanding Cybersecurity Leadership Concepts
- Exploring Control Types and Methods
- Explaining Patch Management Concepts

Exploring Threat Intelligence and Threat Hunting Concepts

- Exploring Threat Actor Concepts
- Identifying Active Threats
- Exploring Threat-Hunting Concepts

Explaining Important System and Network Architecture Concepts

- Reviewing System and Network Architecture Concepts
- Exploring Identity and Access Management (IAM)
- Maintaining Operational Visibility

Understanding Process Improvement in Security Operations

- Exploring Leadership in Security Operations
- Understanding Technology for Security Operations

Implementing Vulnerability Scanning Methods

- Explaining Compliance Requirements
- Understanding Vulnerability Scanning Methods
- Exploring Special Considerations in Vulnerability Scanning

Performing Vulnerability Analysis

- Understanding Vulnerability Scoring Concepts
- Exploring Vulnerability Context Considerations

Communicating Vulnerability Information

- Explaining Effective Communication Concepts

- Understanding Vulnerability Reporting Outcomes and Action Plans

Explaining Incident Response Activities

- Exploring Incident Response Planning
- Performing Incident Response Activities

Demonstrating Incident Response Communication

- Understanding Incident Response Communication
- Analyzing Incident Response Activities

Applying Tools to Identify Malicious Activity

- Identifying Malicious Activity
- Explaining Attack Methodology Frameworks
- Explaining Techniques for Identifying Malicious Activity

Analyzing Potentially Malicious Activity

- Exploring Network Attack Indicators
- Exploring Host Attack Indicators
- Exploring Vulnerability Assessment Tools

Understanding Application Vulnerability Assessment

- Analyzing Web Vulnerabilities
- Analyzing Cloud Vulnerabilities

Exploring Scripting Tools and Analysis Concepts

- Understanding Scripting Languages
- Identifying Malicious Activity Through Analysis

Understanding Application Security and Attack Mitigation Best Practices

- Exploring Secure Software Development Practices
- Recommending Controls to Mitigate Successful Application Attacks
- Implementing Controls to Prevent Attacks