CompTIA CySA+ Certification Training (CS0-003)

O que você aprenderá nesta formação

A formação CompTIA CySA+ foi projetada principalmente para profissionais de segurança cibernética que desempenham funções de trabalho relacionadas à proteção de sistemas de informação garantindo sua disponibilidade, integridade, autenticação, confidencialidade e não repúdio.

Esta formação se concentra no conhecimento, capacidade e habilidades necessárias para fornecer a defesa desses sistemas de informação em um contexto de segurança cibernética, incluindo proteção, detecção, análise, investigação e processos de resposta. Além disso, a formação garante que todos os membros de uma equipa das TICs — todos, desde a equipe do help desk até o Chief Information Officer — entendam seu papel nesses processos de segurança.

O exame de certificação CompTIA Cybersecurity Analyst (CySA+) assegurará que o candidato aprovado tem o conhecimento e as habilidades necessárias para:

- Detectar e analisar indicadores de atividade maliciosa
- Analisar a saída de ferramentas de avaliação de vulnerabilidade
- Analisar dados para priorizar vulnerabilidades
- Entender os conceitos de caça a ameaças e inteligência de ameaças
- Usar ferramentas e métodos apropriados para gerenciar, priorizar e responder a ataques
- Executar processos de resposta a incidentes
- Explicar a importância dos conceitos de arquitetura de sistema e rede em operações de segurança

As ameaças à segurança da informação estão aumentando em todo o mundo, deixando as organizações em busca de analistas de segurança bem treinados. O CySA+ CS0-003 foi atualizado para refletir as tendências atuais em ferramentas de analistas de segurança, como sistemas de Gerenciamento de Informações e Eventos de Segurança Empresarial (SIEM) e EDR/XDR, que amadureceram para incluir mais recursos automatizados. Além disso, o exame CySA+ inclui cobertura expandida de indicadores de comprometimento de nuvem, dispositivos móveis e confiança zero e mais ênfase em tópicos de caça a ameaças, automação de inteligência e priorização de alertas para melhor resposta a incidentes.

A quem se destina

- Analista de Segurança
- Analista do Centro de Operações de Segurança (SOC)
- Administrador de Segurança
- Analista de Resposta a Incidentes
- Analista de Gerenciamento de Vulnerabilidades
- Engenheiro de Segurança

Metodologia, Duração, Preço

Formação via *virtual class* ou presencial com combinação de aulas expositivas e práticas, e simulado, com duração de cinco dias. Kz 1.297.000 por participante, incluindo um voucher para o exame **CS0-003: CompTIA CySA+**.

Pré-requisitos

CompTIA Network+, Security+ ou conhecimento equivalente. Mínimo de 2 anos de experiência prática como analista de resposta a incidentes ou analista de Centro de Operações de Segurança (SOC) ou experiência equivalente.

Conteúdo Programático

Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Understanding Cybersecurity Leadership Concepts
- Exploring Control Types and Methods
- Explaining Patch Management Concepts

Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Exploring Threat Actor Concepts
- Identifying Active Threats
- Exploring Threat-Hunting Concepts

Lesson 3: Explaining Important System and Network Architecture Concepts
- Reviewing System and Network Architecture Concepts
- Exploring Identity and Access Management (IAM)
- Maintaining Operational Visibility

Lesson 4: Understanding Process Improvement in Security Operations
- Exploring Leadership in Security Operations
- Understanding Technology for Security Operations

Lesson 5: Implementing Vulnerability Scanning Methods
- Explaining Compliance Requirements
- Understanding Vulnerability Scanning Methods
- Exploring Special Considerations in Vulnerability Scanning

Lesson 6: Performing Vulnerability Analysis
- Understanding Vulnerability Scoring Concepts
- Exploring Vulnerability Context Considerations

Lesson 7: Communicating Vulnerability Information
- Explaining Effective Communication Concepts
- Understanding Vulnerability Reporting Outcomes and Action Plans

Lesson 8: Explaining Incident Response Activities
- Exploring Incident Response Planning
- Performing Incident Response Activities

Lesson 9: Demonstrating Incident Response Communication
- Understanding Incident Response Communication
- Analyzing Incident Response Activities

Lesson 10: Applying Tools to Identify Malicious Activity

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

Lesson 11: Analyzing Potentially Malicious Activity

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

Lesson 12: Understanding Application Vulnerability Assessment

Analyzing Web Vulnerabilities
Analyzing Cloud Vulnerabilities

Lesson 13: Exploring Scripting Tools and Analysis Concepts

Understanding Scripting Languages
Identifying Malicious Activity Through Analysis

Lesson 14: 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