

CompTIA CySA+ Certification Training (CS0-004)

O que você aprenderá nesta formação

A formação CompTIA Cybersecurity Analyst (CySA+) prepara profissionais para atuar em operações de segurança, gestão de vulnerabilidades e resposta a incidentes. O conteúdo acompanha a versão 4 do exame, série CS0-004, e aborda ambientes locais, em nuvem e híbridos.



Ao longo da formação, os participantes desenvolvem competências para monitorar e analisar dados de segurança, investigar atividades suspeitas, avaliar e priorizar vulnerabilidades e executar processos de resposta a incidentes. A formação também aborda automação, melhoria de processos e uso responsável de inteligência artificial nas operações de segurança.

O exame CompTIA Cybersecurity Analyst (CySA+) CS0-004 valida conhecimentos e competências para:

- Analisar indicadores de atividade maliciosa em redes, dispositivos, aplicações, identidades e ambientes em nuvem
- Utilizar SIEM, EDR, ferramentas de análise de pacotes e plataformas de inteligência de ameaças
- Aplicar conceitos de arquitetura de sistemas e redes, gestão de identidades, registros e monitorização
- Implementar métodos de varredura e interpretar resultados de avaliações de vulnerabilidades
- Priorizar e mitigar vulnerabilidades com base no risco e no contexto do negócio
- Executar processos de resposta a incidentes, incluindo triagem, análise, contenção, erradicação, recuperação e documentação
- Melhorar operações de segurança por meio de automação, orquestração, comunicação eficaz e uso responsável de IA

A versão 4 atualiza os conhecimentos e as competências necessários para as operações de segurança atuais. O exame abrange análise de atividade suspeita em endpoints, redes, aplicações e ambientes de nuvem; gestão de vulnerabilidades orientada ao risco; resposta a incidentes; relatórios e métricas; automação de processos; e conceitos de inteligência artificial, incluindo riscos e governança.

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 em *virtual class* ou presencial, com aulas expositivas, exercícios práticos e simulado, durante cinco dias. Kz 1.297.000 por participante, incluindo um voucher para o exame **CS0-004: 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. Para candidatos ao exame, a CompTIA recomenda cerca de quatro anos de experiência numa função de analista SOC ou de gestão de vulnerabilidades.

Conteúdo Programático

Lição 1: Fundamentos das Operações de Segurança

- Fundamentos de Cibersegurança
- Governança, Políticas e Controlos
- Introdução à Resposta a Incidentes no SOC

Lição 2: Aplicação de Estratégias de Gestão de Risco

- Conceitos de Risco
- Frameworks de Modelação de Ameaças

Lição 3: Gestão da Segurança e das Configurações de Sistemas

- Gestão da Superfície de Ataque
- Fortalecimento de Sistemas (*Hardening*)

Lição 4: Comparação de Arquiteturas de Sistemas

- Infraestrutura e Arquitetura de Sistemas
- Arquiteturas de Redes Modernas
- Infraestruturas Críticas e Controlos Industriais

Lição 5: Aplicação da Gestão de Acessos

- Gestão de Identidade e Acesso
- Gestão de Dispositivos e Endpoints
- Proteção de Dados e Criptografia

Lição 6: Inteligência de Ameaças e Caça a Ameaças

- Conceitos de Agentes de Ameaça
- Fontes de Inteligência de Ameaças
- Caça a Ameaças (*Threat Hunting*)

Lição 7: Avaliação de Vulnerabilidades de Rede

- Fundamentos da Varredura de Vulnerabilidades
- Tipos de Varredura de Vulnerabilidades
- Seleção de Ferramentas para Avaliação de Vulnerabilidades
- Análise e Priorização de Vulnerabilidades
- Relatórios de Vulnerabilidades e Incidentes

Lição 8: Gestão da Resposta a Incidentes e Comunicação

- Gestão de Registos
- Escalonamento de Incidentes
- Atividades Pós-Incidente
- Métricas de Resposta a Incidentes

Lição 9: Execução de Planos de Resposta a Incidentes

- Frameworks de Metodologia de Ataque
- Processo de Resposta a Incidentes
- Técnicas de Resposta a Incidentes

Lição 10: Análise de Atividade Maliciosa

- Ferramentas de Detecção e Análise de Ameaças
- Indicadores de Comprometimento em Hosts
- Indicadores de Comprometimento em Redes
- Indicadores em Aplicações e na Web

Lição 11: Automação da Análise de Dados

- Fundamentos de Scripting
- Linguagens de Scripting
- Análise de Segurança e Reconhecimento de Padrões
- Integração de Tecnologias e Ferramentas

Lição 12: Melhoria de Processos com Automação

- Normalização e Coordenação de Equipas
- Automação, Orquestração e Enriquecimento
- Riscos e Governança da IA
- IA em Operações de Segurança

Lição 13: Avaliação de Vulnerabilidades de Aplicações

- Análise de Vulnerabilidades Web e de Aplicações
- Avaliação de Vulnerabilidades na Nuvem

Lição 14: Segurança de Aplicações

- Desenvolvimento e Testes Seguros de Software
- Identificação e Mitigação de Ataques a Aplicações

CompTIA
Authorized Partner

DELIVERY
PARTNER