CompTIA Cybersecurity Analyst+ CertPrep (CySA+) (e-Learning)

CompTIA

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

Sobre o curso

Aprende a analisar, monitorizar e proteger infraestruturas críticas através de ferramentas de deteção e de análise de ameaças.

Neste curso, os participantes vão adquirir as ferramentas e as táticas necessárias para gerir riscos de cibersegurança, identificar vários tipos de ameaças comuns, avaliar a segurança de uma organização, recolher e analisar a inteligência de cibersegurança e lidar com incidentes à medida que estes vão ocorrendo. Este curso oferece uma abordagem abrangente à segurança, voltada para aqueles que estão na linha da frente da defesa da cibersegurança.

Este curso foi desenvolvido para ajudar os participantes a prepararem-se para o exame de certificação CompTIA CySA+ Cybersecurity Analyst+.

CySA+ da CompTIA é uma certificação global, independente de fornecedor, que abrange o conhecimento e as competências de nível intermédio exigidas aos analistas de segurança da informação. A posse da mesma ajuda a comprovar a capacidade de um profissional de cibersegurança de defender, de forma proativa, uma organização através de procedimentos de monitorização, de identificação de ameaças, de resposta a incidentes e do trabalho em equipa.

O exame de certificação CompTIA CySA+ garante que o candidato é detentor do conhecimento e das competências para:

- Detetar e analisar indicadores de atividade maliciosa
- Compreender conceitos de caça a ameaças e inteligência de ameaças
- Utilizar ferramentas e métodos adequados para gerir, priorizar e responder a ataques e vulnerabilidades
- Executar processos de resposta a incidentes
- Compreender conceitos de reporting e comunicação relacionados com a gestão de vulnerabilidades e atividades de resposta a incidentes

Este curso e-learning inclui:

- **Conteúdos formativos estruturados em e-learning:** Aprende e desenvolve competências de forma eficiente e autónoma, com conteúdos estruturados através de um modelo de progressão da

aprendizagem. Este modelo ajuda-te a compreender conceitos e a desenvolver competências alinhadas com os objetivos do curso.
- **Vídeos e conteúdos interativos integrados:** Acede a explicações, demonstrações e exemplos no momento em que são mais relevantes para a tua aprendizagem.
- **Atividades em laboratório:** Realiza exercícios práticos em ambientes simulados e reais, com cenários próximos do contexto profissional e tarefas de nível básico e avançado.
- **Assessments e testes de preparação:** Valida os teus conhecimentos ao longo do curso através de avaliações e testes práticos.
- **Voucher de exame e retake:** Inclui voucher de exame de certificação e a possibilidade de repetição em caso de reprovação.

Destinatários

- Analistas de Segurança de TI
- Analistas de Centro de Operações de Segurança (SOC)
- Analistas de Vulnerabilidades
- Especialistas de Cibersegurança
- Threat Intelligence Analysts
- Engenheiros de Segurança Informática

Objetivos

- Explicar a importância dos controlos de segurança e da inteligência de segurança
- Utilizar dados e inteligência de ameaças
- Analisar dados de monitorização de segurança
- Recolher e consultar dados de monitorização de segurança
- Utilizar técnicas de análise forense digital e de análise de indicadores
- Aplicar procedimentos de resposta a incidentes
- Aplicar frameworks de mitigação de riscos e de segurança
- Executar a gestão de vulnerabilidades
- Aplicar soluções de segurança para gestão de infraestruturas
- Compreender privacidade e proteção de dados
- Aplicar soluções de segurança para garantia de software
- Aplicar soluções de segurança para cloud e automação

Condições

Notas

Após a formação, é possível adquirir, na Rumos, o exame de certificação do parceiro oficial com 10% de desconto.

Oferta válida até 6 meses após a conclusão do curso nas modalidades live training ou presencial.

Para particulares

• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Possibilidade de pagamento faseado.
• Possibilidade de beneficiar do Cheque Formação+Digital até 750€ (conforme elegibilidade).
• Isenção de IVA para particulares.

Para empresas

• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).
• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

A fim de garantir uma participação bem-sucedida neste curso, os participantes deverão atender aos seguintes pré-requisitos:

- Recomenda-se pelo menos dois anos de experiência em tecnologia de segurança de redes de computadores ou numa área relacionada.
- Capacidade de reconhecer vulnerabilidades e ameaças de segurança da informação no contexto da gestão de riscos.
- Competências operacionais de nível básico com alguns dos sistemas operativos mais comuns para ambientes de computação.
- Conhecimentos básicos dos conceitos e do quadro operacional das medidas de salvaguarda mais comuns em ambientes de computação. As medidas incluem autenticação e autorização básicas, permissões de recursos e mecanismos antimalware, entre outros.
- Compreensão básica de alguns dos conceitos mais comuns relacionados com ambientes de rede, como roteamento e switching.
- Conhecimentos básicos dos principais protocolos de redes TCP/IP, incluindo TCP, IP, UDP, DNS, HTTP, ARP, ICMP, DHCP, entre outros.
- Conhecimentos básicos dos conceitos e do quadro operacional das medidas de salvaguarda mais comuns em ambientes de rede. As medidas incluem firewalls, sistemas de prevenção de intrusões, VPNs, entre outros.

Metodologia

e-learning

Programa

- Compreensão da Resposta, do Tratamento e da Gestão de Vulnerabilidades
- Conceitos de Inteligência de Ameaças e Caça a Ameaças
- Explicação de Conceitos Importantes de Arquitetura de Sistemas e Redes
- Compreensão da Melhoria de Processos nas Operações de Segurança
- Implementação de Métodos de Deteção de Vulnerabilidades
- Realização de Análise de Vulnerabilidades
- Comunicação de Informações sobre Vulnerabilidades
- Explicação de Atividades de Resposta a Incidentes
- Comunicação de Resposta a Incidentes
- Aplicação de Ferramentas de Identificação de Atividade Maliciosa
- Análise de Atividades Potencialmente Maliciosas
- Compreensão da Avaliação de Vulnerabilidades de Aplicações
- Ferramentas de Scripting e Conceitos de Análise
- Compreensão de Boas Práticas de Segurança de Aplicações e de Mitigação de Ataques

Compreensão da Resposta, do Tratamento e da Gestão de Vulnerabilidades

- Compreender os Conceitos de Liderança em Cibersegurança
- Explorar Tipos e Métodos de Controlo
- Explicar Conceitos de Gestão de Patches

Conceitos de Inteligência de Ameaças e Caça a Ameaças

- Explorar Conceitos de Atores de Ameaças
- Identificar Ameaças Ativas
- Explorar Conceitos de Caça a Ameaças

Explicação de Conceitos Importantes de Arquitetura de Sistemas e Redes

- Revisão de Conceitos de Arquitetura de Sistemas e Redes
- Explorar Gestão de Identidade e de Acesso (IAM)
- Manter Visibilidade Operacional

Compreensão da Melhoria de Processos nas Operações de Segurança

- Explorar a Liderança nas Operações de Segurança
- Compreender a Tecnologia para Operações de Segurança

Implementação de Métodos de Deteção de Vulnerabilidades

- Explicar Requisitos de Conformidade
- Compreender Métodos de Deteção de Vulnerabilidades
- Explorar Considerações Especiais ao Detetar Vulnerabilidades

Realização de Análise de Vulnerabilidades

- Compreender Conceitos de Pontuação de Vulnerabilidades
- Explorar Considerações sobre o Contexto de Vulnerabilidades

Comunicação de Informações sobre Vulnerabilidades

- Explicar Conceitos de Comunicação Eficaz
- Compreender Resultados e Planos de Ação dos Relatórios de Vulnerabilidades

Explicação de Atividades de Resposta a Incidentes

- Explorar o Plano de Resposta a Incidentes
- Realizar Atividades de Resposta a Incidentes

Comunicação de Resposta a Incidentes

- Compreender a Comunicação de Resposta a Incidentes
- Analisar Atividades de Resposta a Incidentes

Aplicação de Ferramentas de Identificação de Atividade Maliciosa

- Identificar Atividade Maliciosa
- Explicar Frameworks Metodológicos de Ataques
- Explicar Técnicas de Identificação de Atividade Maliciosa

Análise de Atividades Potencialmente Maliciosas

- Explorar Indicadores de Ataques a Redes
- Explorar Indicadores de Ataques a Hosts
- Explorar Ferramentas de Avaliação de Vulnerabilidades

Compreensão da Avaliação de Vulnerabilidades de Aplicações

- Analisar Vulnerabilidades na Web
- Analisar Vulnerabilidades na Cloud

Ferramentas de Scripting e Conceitos de Análise

- Compreender Linguagens de Scripting
- Identificar Atividade Maliciosa Através de Análise

Compreensão de Boas Práticas de Segurança de Aplicações e de Mitigação de Ataques

- Explorar Práticas de Desenvolvimento de Software Seguro
- Recomendar Dispositivos de Controlo para Mitigação de Ataques a Aplicações
- Implementar Dispositivos de Controlo para Prevenção de Ataques