Check Point Security Administrator R82 (CCSA)

Check Point

- **Nível:** Intermédio
- **Duração:** 21h

Sobre o curso

Este curso fornece aos formandos os conhecimentos fundamentais, as competências e a experiência prática necessários para configurar, gerir e monitorizar um ambiente Quantum Security existente.

Os formandos irão aprender a aceder e navegar no Gaia Portal e na Gaia Command Line Interface, a gerir o acesso de administradores, criar e configurar Network Objects, criar novas Security Policies, configurar Ordered Layers e uma Shared Inline Layer, visualizar o tráfego e monitorizar o estado do sistema, configurar Identity Awareness, reforçar a segurança com HTTPS Inspection, configurar Application Control e URL Filtering, e configurar Autonomous Threat Prevention.

Destinatários

- Administradores de Segurança
- Engenheiros de Segurança
- Analistas de Segurança
- Consultores de Segurança
- Arquitetos de Segurança

Condições

Após a formação, é possível adquirir, o exame de certificação do parceiro oficial com 10% de desconto. Oferta válida até 6 meses após a conclusão do curso.

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.
• Possibilidade de pagamento em até 12 prestações mensais sem juros via Cofidis Pay (até 2.500€, sujeito a aprovação).
• 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

- Unix e/ou Windows OS
- Fundamentos de Internet
- Fundamentos de Redes
- Segurança em Redes
- Administração de Sistemas
- Redes TCP/IP

Metodologia

- Sessões teóricas e práticas.

Programa

- Introdução ao Quantum Security
- Gestão de Contas de Administrador
- Gestão de Objetos
- Gestão de Políticas de Segurança
- Policy Layers
- Monitorização de Operações de Segurança
- Identity Awareness
- HTTPS Inspection
- Application Control e URL Filtering
- Fundamentos de Threat Prevention

Introdução ao Quantum Security

- Identificar os principais componentes da Check Point Three-Tier Architecture e explicar como funcionam em conjunto no ambiente Check Point.

Laboratórios:

- Explorar o Gaia no Security Management Server
- Explorar o Gaia no Dedicated Log Server
- Explorar o Gaia nos Security Gateway Cluster Members
- Ligar ao SmartConsole
- Navegar nas vistas GATEWAYS & SERVERS

- Navegar nas vistas SECURITY POLICIES
- Navegar nas vistas LOGS & EVENTS
- Navegar nas vistas MANAGE & SETTINGS

Gestão de Contas de Administrador

- Explicar o propósito das contas de administrador do SmartConsole.
- Identificar funcionalidades úteis para a colaboração entre administradores, como session management, concurrent administration e concurrent policy installation.

Laboratórios:

- Criar novos administradores e atribuir perfis
- Testar atribuições de perfis de administrador
- Gerir sessões concorrentes de administradores
- Assumir outra sessão e verificar o estado da sessão

Gestão de Objetos

- Explicar o propósito dos SmartConsole Objects.
- Dar exemplos de SmartConsole Physical e Logical Objects.

Laboratórios:

- Visualizar e modificar GATEWAYS & SERVERS Objects
- Visualizar e modificar Network Objects
- Visualizar e modificar Service Objects

Gestão de Políticas de Segurança

- Explicar o propósito das Security Policies.
- Identificar os elementos essenciais de uma Security Policy.
- Identificar funcionalidades e capacidades que melhoram a configuração e gestão da Security Policy.

Laboratórios:

- Verificar a Security Policy
- Modificar Security Policies
- Instalar a Standard Security Policy
- Testar a Security Policy

Policy Layers

- Demonstrar compreensão do conceito de policy layer da Check Point.
- Explicar como as policy layers afetam a inspeção de tráfego.

Laboratórios:

- Adicionar uma Ordered Layer
- Configurar e aplicar as regras da Ordered Layer

- Testar a Ordered Layer Policy
- Criar uma Inline DMZ Layer
- Testar a Inline DMZ Layer

Monitorização de Operações de Segurança

- Explicar o propósito da Security Operations Monitoring.
- Ajustar a configuração do Log Server.
- Utilizar queries predefinidas e personalizadas para filtrar os resultados de logging.
- Monitorizar o estado dos sistemas Check Point.

Laboratórios:

- Configurar Log Management
- Melhorar a visualização da Rulebase, Regras e Logging
- Rever logs e pesquisar dados
- Configurar o Monitoring Blade
- Monitorizar o estado dos sistemas

Identity Awareness

- Explicar o propósito da solução Identity Awareness.
- Identificar os elementos essenciais do Identity Awareness.

Laboratórios:

- Ajustar a Security Policy para Identity Awareness
- Configurar o Identity Collector
- Definir o User Access Role
- Testar o Identity Awareness

HTTPS Inspection

- Explicar o propósito da solução HTTPS Inspection.
- Identificar os elementos essenciais do HTTPS Inspection.

Laboratórios:

- Ativar o HTTPS Inspection
- Ajustar as Access Control Rules
- Implementar o certificado do Security Gateway
- Testar e analisar a policy com HTTPS Inspection

Application Control e URL Filtering

- Explicar o propósito das soluções Application Control e URL Filtering.
- Identificar os elementos essenciais de Application Control e URL Filtering.

Laboratórios:

- Ajustar a Access Control Policy
- Criar e ajustar Application Control e URL Filtering
- Testar e ajustar as regras de Application Control e URL Filtering

Fundamentos de Threat Prevention

- Explicar o propósito da solução Threat Prevention.
- Identificar os elementos essenciais do Autonomous Threat Prevention.

Laboratórios:

- Ativar o Autonomous Threat Prevention
- Testar o Autonomous Threat Prevention