

Check Point Security Engineering R80.20 (CCSE)

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Lisboa
- **Data:** 13 Out. 2020 a 15 Out. 2020
- **Preço:** 1990€
- **Horário:** Laboral - das 09h00 às 17h00
- **Nível:** Avançado
- **Duração:** 21 horas

Neste curso avançado de 3 dias poderá aprender a construir, modificar, implementar e resolver problemas nos sistemas de segurança da Check Point baseados na plataforma GAiA.

Laboratórios permitirão fazer debug aos processos da firewall, otimizar a performance das VPN e realizar upgrades às plataformas de Management, entre outras tarefas.

Destinatários

Expert users and resellers who need to perform advanced deployment configurations of Check Point Software Blades, which includes:

- System administrators
- Support analysts
- Network engineers
- Anyone seeking CCSE certification

Pré-requisitos

- CCSA training/certification
- Working knowledge of Windows, UNIX, networking, TCP/IP, and the Internet

Objectivos

Validate your understanding and skills necessary to configure and optimally manage Check Point Next Generation Firewalls:

- Identify advanced CLI commands.
 - Understand system management procedures, including how to perform system upgrades and apply patches and hotfixes.
 - Describe the Check Point Firewall infrastructure.
 - Describe advanced methods of gathering important gateway data using CPView and CPInfo.
 - Recognize how Check Point's flexible API architecture supports automation and orchestration.
 - Discuss advanced ClusterXL functions.
 - Describe VRRP network redundancy advantages.
 - Understand how SecureXL acceleration technology is used to enhance and improve performance.
 - Understand how CoreXL acceleration technology is used to enhance and improve performance.
 - Identify the SmartEvent components that store network activity logs and identify events.
 - Discuss the SmartEvent process that determines which network activities may lead to security issues.
 - Understand how SmartEvent can assist in detecting, remediating, and preventing security threats.
 - Discuss the Mobile Access Software Blade and how it secures communication and data.
 - Understand Mobile Access deployment options.
 - Recognize Check Point Remote Access solutions.
 - Discuss Check Point Capsule components and how they protect mobile devices and business documents.
 - Discuss different Check Point Solutions for attacks such as zero-day and Advanced Persistent Threats.
 - Understand how SandBlast, Threat Emulation, and Threat Extraction prevent security incidents.
 - Identify how Check Point Mobile Threat Prevention can help protect data accessed on company-issued smartphones and tablets.
-

Metodologia

- Sessões teóricas e práticas.
-

Programa

LAB EXERCISES

- Upgrading a Security Management Server to R80.X
- Applying Check Point Hotfixes
- Configuring a New Security Gateway Cluster
- Core CLI Elements of Firewall Administration
- Configuring Manual Network Address Translation
- Managing Objects Using the Check Point API
- Enabling Check Point VRRP
- Deploying a Secondary Security Management Server
- Viewing the Chain Modules
- Working with SecureXL
- Working with CoreXL
- Evaluating Threats with SmartEvent
- Managing Mobile Access

- Understanding IPS Protections
- Deploying IPS Geo Protection
- Reviewing Threat Prevention Settings and Protections
- Deploying Threat Emulation and Threat Extraction