Rumos valorizamos profissionais!

Check Point Administrator and Troubleshooting R81.10 (CCSA+CCTA)

- **Formato do curso:** Presencial
- **Localidade:** Lisboa
- **Data:** 21 Fev. 2022 a 25 Fev. 2022
- **Preço:** 2650€
- **Horário:** Laboral - das 9h00 às 17h00
- **Duração:** 35 horas

This 5-day course combines the Check Point Security Administrator (CCSA) and the Check Point Troubleshooting Administrator (CCTA) courses.

This course covers:

- everything you need to start-up, configure and manage daily operations of R81.10 Check Point Security Gateway and Management Software Blades systems on the GAiA operating system.
- the concepts and skills necessary to troubleshoot and investigate issues that may occur when managing the Check Point Security Management architecture and Security Gateways.

Destinatários

- Technical persons who support, install, deploy, administer and troubleshoot Check Point Software Blades. This could include the following:
  - System administrators
  - Support analysts
  - Security managers
  - Network engineers

Pré-requisitos

- General knowledge of TCP/IP
- Working knowledge of Windows, UNIX, network technology, and the Internet

Metodologia

- Sessões teóricas e práticas.

Programa

LAB EXERCISES ADMINISTRATION

- Configure the Security Management Server.
- Use the WebUI to run the First Time Wizard.
- Install the Smart Console.
- Install the Alpha Gateway using the network detailed in the course topology.
- Demonstrate how the Security Management Server and Gateway communicate.
- Test SIC Status.
- Create multiple administrators and apply different roles and permissions for simultaneous administration.
- Validate existing licenses for products installed on the network.
- Create and configure host, network and group objects.
- Create a simplified Security Policy.
- Demonstrate how to use Security Zones in policy.
- Demonstrate how to share a layer between Security Polices.
- Configure Network Address Translation for server and network objects.
- Enable Identity Awareness.
- Deploy user access roles for more granular control of the security Policy.
- Generate network Traffic and use traffic visibility tools to monitor the data.
- Use SmartConsole and SmartView Monitor to view status, alerts, and block suspicious traffic.

LAB EXERCISES TROUBLESHOOTING

- Using tcpdump and Wireshark
- Viewing Firewall Chain Modules
- Using Basic Linux and Check Point Commands
- Troubleshooting Logging Communication Issues
- Analyzing Traffic Captures
- Troubleshooting SmartConsole and Using SmartConsole Tools
- Troubleshooting Identity Awareness
- Troubleshooting Application Control and URL Filtering
- Investigating Network Address Translation Issues
- Evaluating Advanced Threat Prevention Products
- Verifying Licenses