# CCSE - Certified Security Expert R81.20 (CCSE)

Check Point - Check Point - Cyber Security

| Durata: | Lingue: | Certificazione: |
| --- | --- | --- |
| **3 Giorni** | **Italiano** | **-** |

**ITCore Group**

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
www.itcoregroup.com

## Descrizione del corso

The CCSE course builds upon and expands the knowledge gained in the CCSA course. It is designed for technicians who need to install, administer, or support Check Point Quantum Gateway products and their management. Participants will learn concepts and develop a deeper understanding of the skills necessary to administer IT security tasks, both fundamental and advanced.
The course includes theoretical aspects as well as practical exercises, ensuring a comprehensive learning experience.

**PREREQUISITES**

CCSA Training or Certification, fundamental Unix and Windows knowledge, certificate management experience, system administration and networking knowledge.

**OBJECTIVES**

• Identify basic interfaces used to manage the Check Point environment.
• Identify the types of technologies that Check Point supports for automation.
• Explain the purpose of the Check Management High Availability (HA) deployment.
• Identify the workflow followed to deploy a Primary and solution Secondary servers.
• Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, connection stickyness.
• Identify how to exclude services from synchronizing or delaying synchronization.
• Explain the policy installation flow.
• Explain the purpose of dynamic objects, updatable objects, and network feeds.
• Understand how to manage user access for internal and external users.
• Describe the Identity Awareness components and configurations.
• Describe different Check Point Threat Prevention solutions.
• Articulate how the Intrusion Prevention System is configured.
• Obtain knowledge about Check Point’s IoT Protect.
• Explain the purpose of Domain-based VPNs.
• Describe situations where externally managed certificate authentication is used.
• Describe how client security can be provided by Remote Access.
• Discuss the Mobile Access Software Blade.
• Explain how to determine if the configuration is compliant with the best practices.
• Define performance tuning solutions and basic configuration workflow.
• Identify supported upgrade and migration methods and procedures for Security Management Servers and dedicated Log and SmartEvent Servers.
• Identify supported upgrade methods and procedures for Security Gateways

## Programma

- Navigate the Environment and Using the Management API
- Deploy Secondary Security Management Server
- Configure a Dedicated Log Server
- Deploy SmartEvent
- Configure a High Availability Security Gateway Cluster
- Work with ClusterXL
- Configure Dynamic and Updateable Objects
- Verify Accelerated Policy Installation and Monitoring Status
- Elevate Security with HTTPS Inspection
- Deploy Identity Awareness
- Customize Threat Prevention
- Configure a Site-to-Site VPN with an Interoperable Device
- Deploy Remote Access VPN
- Configure Mobile Access VPN
- Monitor Policy Compliance
- Report SmartEvent Statistics
- Tuning Security Gateway Performance