

DEFINE. DESIGN. DELIVER.

# CHECK POINT CERTIFIED SECURITY EXPERT (CCSE) R80



COURSE PREPARES  
FOR EXAM:

#156-315.80



## WHO SHOULD ATTEND?

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



## COURSE GOAL

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



## COURSE PREREQUISITES

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



## Course Topics

- System Management
- Automation and Orchestration
- Redundancy
- Acceleration
- SmartEvent
- Mobile and Remote Access
- Threat Prevention

## Course Objectives

- 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.

## Lab Exercises

- Upgrading a Security Management Server to R80.10
- 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

PenteseC are an Authorised Training Centre for Check Point. To find out more, contact us today:

Call 0845 519 1337 or Email [sales@penteseC.com](mailto:sales@penteseC.com)