Document Generated: 10/28/2025

Learning Style: Virtual Classroom

Technology: Citrix

Difficulty: Intermediate

Course Duration: 3 Days

Check Point Certified Security Expert (R81.x)

About this Course:

The Check Point Certified Security Expert (CCSE) R81.x course is an advanced training program designed to provide participants with the skills needed to build, modify, deploy, and troubleshoot Check Point Security systems on the Gaia OS. This course includes a mix of lectures and hands-on lab exercises to ensure

practical understanding and application.

Course Objectives:

By the end of this course, participants will be able to:

- Configure and manage Check Point Security Gateway and Management Software Blades.
- Perform advanced troubleshooting and problem resolution.
- Implement advanced VPN concepts and configurations.
- Optimize VPN performance and troubleshoot VPN issues.
- Understand and configure advanced security policies and settings.

Audience:

This course is intended for:

- Security administrators.
- Network engineers.
- IT professionals responsible for managing Check Point Security solutions.
- Individuals preparing for the Check Point Certified Security Expert (CCSE) certification.

Prerequisites:

Participants should have:

- Completed the Check Point Certified Security Administrator (CCSA) course or have equivalent knowledge.
- Basic knowledge of networking concepts.
- Familiarity with Windows and UNIX operating systems.
- If you need more details or have any specific questions about the course, feel free to ask!

Course Outline:

1. Advanced System Management
    - Advanced CLI commands
    - System upgrades, patches, and hotfixes
    - Gathering gateway data using CPView and CPInfo
2. Automation and Orchestration
    - Check Point API architecture
    - Automating tasks and orchestrating workflows

3. Advanced Security Gateway and Management Configurations
    - Advanced Firewall infrastructure
    - Security policies and settings
    - Threat prevention and management

4. Redundancy and Acceleration
    - ClusterXL advanced functions
    - VRRP network redundancy
    - SecureXL and CoreXL acceleration technologies

5. SmartEvent and Logging
    - SmartEvent components and network activity logs
    - Identifying and responding to security events
    - Using SmartEvent for threat detection and prevention

6. Mobile and Remote Access
    - Mobile Access Software Blade
    - Securing communication and data
    - Deployment options for mobile access

7. Threat Prevention
    - SandBlast, Threat Emulation, and Threat Extraction
    - Protecting against zero-day attacks and Advanced Persistent Threats (APTs)
    - Check Point Capsule components for mobile security

8. Advanced VPN Concepts
    - VPN performance optimization
    - Troubleshooting VPN issues
    - Implementing advanced VPN configurations