CCSA+CCSE Check Point Cybersecurity Boot Camp (CCSA+CCSE)

Price	Duration	Delivery Methods
$5,000.00	5 Days	VILT, Private Group

This special CCSA and CCSE bundle covering Check Point Certified Security Administrator and Security Expert content (R80.40) validates and enhances your skills to manage Check Point advanced security management systems and to administer IT security fundamental tasks.

Who Should Attend

This special combo or bundle course is recommended for Systems Administrators, Network Engineers, Security Managers, Support Analysts and any other IT professional working with Check Point Software Blades or seeking CCSA and CCSE certifications.

Course Objectives

- Security Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contracts
- Policy Rules and Rulebase
- Policy Package
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia
- Permissions
- Policy Installation
- Advanced Deployments
- Management High Availability
- Advanced Gateway Deployment
- Advanced Policy Configuration
- Advanced User Access Management
- Custom Threat Protection
- Advanced Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Advanced Security Monitoring
- Advanced Security Maintenance

Agenda

- 1. Security Administrator
- 2. Objectives
- 3. Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- 4. Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution
- 5. Create SmartConsole objects that correspond to the organization?s topology for use in policies and rules.
- 6. Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- 7. Identify features and capabilities that enhance the configuration and management of the Security Policy.
- 8. Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization?s security requirements.

- 9. Describe how to analyze and interpret VPN tunnel traffic.
- 10. Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- 11. Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method.
- 12. Identify the types of technologies that Check Point supports for automation.
- 13. Explain the purpose of the Check Management High Availability (HA) deployment.
- 14. Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, and connection stickyness.
- 15. Explain the purpose of dynamic objects, updatable objects, and network feeds.
- 16. Describe the Identity Awareness components and configurations.
- 17. Describe different Check Point Threat Prevention solutions.
- 18. Articulate how the Intrusion Prevention System is configured.
- 19. Explain the purpose of Domain-based VPNs
- 20. Describe situations where externally managed certificate authentication is used.
- 21. Describe how client security can be provided by Remote Access.
- 22. Discuss the Mobile Access Software Blade.
- 23. Define performance tuning solutions and basic configuration workflow.
- 24. Identify supported upgrade methods and procedures for Security Gateways.