CHECK POINT

CCSA & CCSE BOOTCAMP

A fast paced five-day class. Participants will gain a comprehensive understanding of concepts with advanced skills training for managing cybersecurity operations using Check Point technology.

Audience

Technical professionals and expert users who support, administer or perform advanced deployment configurations of Check Point Products

Goals

Learn basic and advanced concepts and the skills necessary to administer IT security fundamental and intermediate tasks

Prerequisites

One-year experience on Check Point products. Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP is recommended

TOPICS

- SECURITY ARCHITECTURE
- FIREWALL BASICS
- THREAT DETECTION
- MANAGEMENT MAINTENANCE
- THE FIREWALL KERNEL
- THREAT PREVENTION
- GAIA PORTAL
- SECURITY EVENTS
- HIDE/STATIC NAT
- ADMIN OPERATIONS
- MONITORING STATES
- POLICY LAYERS
- MANAGEMENT MIGRATION
- USER-MODE PROCESSES
- THREAT EMULATION
- USER ACCESS
- POLICY AUTOMATION
- DEPLOYMENT
- CLUSTERXL
- SITE-TO-SITE VPN
- MANAGEMENT
- CLUSTERXL
- ADVANCED SITE-TO-SITE VPN
- CORE ACCELERATION
- MOBILE ACCESS
- LICENSING
- TRAFFIC VISIBILITY
- REMOTE ACCESS VPN
- HIGH AVAILABILITY
- TRAFFIC ACCELERATION
- REMOTE ACCESS VPN
- COMPLIANCE TASKS
- GATEWAY MAINTENANCE
- INTERFACE ACCELERATION

SECURITY ADMINISTRATOR

Objectives

- Know how to perform periodic administrator tasks.
- Describe the basic functions of the Gaia operating system.
- Recognize SmartConsole features, functions, and tools.
- Describe the Check Point Firewall infrastructure.
- Understand how SmartConsole is used by administrators to grant permissions and user access.
- Learn how Check Point security solutions and products work and how they protect networks.
- Understand licensing and contract requirements for Check Point security products.

Exercises

- Identify key components and configurations.
- Create and confirm administrator users for the domain.
- Validate existing licenses for products installed on your network.
- Create and modify Check Point Rule Base objects.
- Demonstrate how to share a layer between Security Policies.
- Analyze network traffic and use traffic visibility tools.
- Monitor Management Server States using SmartConsole.

SECURITY EXPERT

Objectives

- Articulate Gaia system management procedures.
- Understand system management procedures, including how to perform system upgrades and how to install 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.
- Understand how SecureXL acceleration technology is used to enhance and improve performance.

Exercises

- Upgrading a Security Management Server.
- Perform Check Point Online Jumbo Hotfixes.
- Migrate a Security Management Server.
- Configuring a New Security Gateway Cluster.
- Core CLI Elements of Firewall Administration.
- Configuring Manual Network Address Translation.
- Managing Objects Using the Check Point API.

CERTIFICATION Prepare for exams #156-215.80.40/#156-315.80 VUE.com/checkpoint

COURSE RECOMMENDATIONS

IDEAL STUDENT PROFILE

» **Previous Experience Recommended**
Students with knowledge of managing cybersecurity operations or Check Point products is recommended.

PRIORITIZED TOPICS

» **Fundamental Chapters** ●
Course content and labs with essential concepts and skills training.

BOOTCAMP CHAPTERS

» CCSA

» Chapter 1: Introduction to Check Point Deployment

» Chapter 3: Check Point Management Operations ●

» Chapter 4: Licensing

» Chapter 5: Security Policy Management ●

» Chapter 6: Policy Layers ●

» Chapter 7: Managing User Access

» Chapter 8: Working with NAT

» Chapter 9: Traffic Visibility

» Chapter 10: Monitoring System States

» Chapter 11: Security Events

» Chapter 12: Basic Concepts of VPN ●

» Chapter 13: Working with ClusterXL ●

» Chapter 14: Compliance Tasks

» CCSE

» Chapter 15: Management Maintenance ●

» Chapter 16: Management Migration ●

» Chapter 17: Management Redundancy ●

» Chapter 18: Automation and Orchestration

» Chapter 19: Gateway Maintenance ●

» Chapter 20: Firewall Kernel ●

» Chapter 21: User Mode Processes ●

» Chapter 22: Gateway Redundancy ●

» Chapter 23: Traffic Acceleration ●

» Chapter 24: Core Acceleration ●

» Chapter 25: Interface Acceleration

» Chapter 26: Threat Prevention ●

» Chapter 27: Threat Emulation ●

» Chapter 28: Advanced Site-to-Site VPN

» Chapter 29: Remote Access

» Chapter 30: Mobile Access