COURSE OUTLINE

Course Name: Cybersecurity Boot camp

DURATION	SKILL LEVEL	DELIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
3 Day(s)	Advanced	In Class/ VITL	Check Point Learning Credits (CLC)	Check Point

Course Overview

Learn basic and advanced concepts and develop skills necessary to administer IT security fundamental

Prerequisite

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

Audience

Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP.

Objectives

Security administrator

- 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.

Security Expert

- 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 SecureX acceleration technology is used to enhance and improve performance.

At Course Completion

- Provide an overview of the upgrade service and options available.

- Explain how to perform management upgrade and migration.

- Articulate the process using CPUSE features.

- Articulate the purpose and function of Management High Availability.

- Explain Primary vs Secondary, Active vs Standby and Synchronization.

- Explain disaster recovery steps in case the primary management server becomes unavailable.

- Provide overview of Central Deployment in SmartConsole.

- Articulate an understanding of Security Gateway cluster upgrade methods.

- Explain about Multi Version Cluster (MVC) upgrades.

- Discuss Gaia Commands and how they are used.

- Explain the main processes on Security Management Servers and Security Gateways.

- Describe how to work with scripts and SmartTasks to configure automatic actions.

- Explain the Management Data Plane Separation (MDPS)

- Explain kernel operations and traffic flow

- Articulate Dynamic and Updatable Objects in Security Gateways

- Explain the policy installation flow and files used.

- Describe the use of policy installation history.

- Explain concurrent and accelerated install policy.

- Describe an overview of APIs and ways to use and authenticate.

- Explain how to make changes in GAIA and management configuration.

- Explain how to install policy using API.

- Explain how the SecureXL acceleration technology enhances and optimizes Security Gateway performance.

- Describe how the CoreXL acceleration technology enhances and improves Security Gateway performance.

- Articulate how utilizing multiple traffic queues can make traffic handling more efficient.

- Discuss Site-to-Site VPN basics, deployment and communities.

- Describe how to analyze and interpret VPN tunnel traffic.

- Explain Link Selection and ISP Redundancy options.

- Explain tunnel management features.

- Discuss Check Point Remote Access solutions and how they differ from each other.

- Describe how client security can be provided by Remote Access .

- Explain authentication methods including machine authentication.

- Explain Multiple Entry Point (MEP).

- Discuss the Mobile Access Software Blade and how it secures communication and data exchange during remote connections.

- Describe Mobile Access deployment options.

- Discuss various features in Mobile Access like Portals, Link Translation, running Native Applications, Reverse Proxy and more.

- Explain basic concepts of Clustering and ClusterXL.

- Explain about Cluster Control Protocol (CCP) and synchronization.

- Describe advanced ClusterXL functions and modes like Load Sharing, Active-Active, VMAC mode etc.

- Discuss Cluster Correction Layer (CCL) to provide connection stickyness.

- Advanced Logs and Monitoring

- Explain how to determine if the configuration is compliant with the best practices.

- Explain how to set action items to meet the compliance.

- Discuss how SmartEvent functions to identify critical security issues.

- Describe the components of SmartEvent and their deployment options.

- Discuss how SmartEvent can assist in reporting security threats.

- Explain how to customize event definitions and set an Event Policy.

Topics

SECURITY ARCHITECTURE

FIREWALL BASICS

THREAT DETECTION

MANAGEMENT MruNTENANCE

THE FIREWALL KERNEL

THREAT PREVENTION

GAIA POR TAL

SECURITY EVENTS

HIDE/STATIC NAT

ADMIN OPERATIONS

MONITORING STATES

POLICY LAYERS

MANAGEMENT MIGRATION

USER-MODE PROCESSES

THREAT EMULATION

USER ACCESS

POLICY AUTOMATION

LICENSING

TRAFFIC VISIBILITY

REMOTE ACCESS VPN

HIGH AVAILABILITY

TRAFFIC ACCELERATION

COMPLIANCE TASK

GATEWAY MAINTANANCE

INTERFACE ACCELERATION

Exams and Certifications

Notes and Annotations

What is Next