# COURSE TOPICS

**CHECK POINT TROUBLESHOOTING EXPERT (CCTE)**

**WHO SHOULD ATTEND?**

This course is designed for security experts and checkpoint resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments.

**COURSE GOAL:**

Provide advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point Security environment.

**PREREQUISITES:**

* Working knowledge of UNIX and/or Windows operating systems
* Working knowledge of Networking TCP/IP
* CCSE training/certification
* Advanced knowledge of Check Point Security products
* Advanced Troubleshooting
* Management Database and Processes
* Advanced Kernel Debugging
* User Mode Troubleshooting
* Advanced Access Control
* Understanding Threat Prevention
* Advanced VPN Troubleshooting
* Acceleration and performance tuning

# LAB EXERCISES

* Monitoring Network Traffic
* Debugging Management Processes
* Exploring the Postgres and Som Databases
* Troubleshooting Management Synchronization
* Analyzing Traffic Issues Using Kernel Debugs
* Debugging User Mode Processes
* Troubleshooting Application Control and URL Filtering
* Troubleshooting IPS
* Evaluating Threat Prevention Products
* Debugging Site-to-Site VPN
* Troubleshooting Remote Access VPN
* Testing Mobile Access VPN
* Evaluating SecureXL
* Modifying CoreXL
* Evaluating Hardware-related Performance
* Tuning and Software Optimization

Website: [**https://datacipher.com/**](https://datacipher.com/)

Email: **training@datacipher.com**

# COURSE OBJECTIVES

* Understand how to use Check Point diagnostic tools to determine the status of a network.
* Understand how to use network packet analyzers and packet

capturing tools to evaluate network traffic.

* Become familiar with more advanced Linux system commands.
* Obtain a deeper knowledge of the Security Management architecture.
* Understand how the Management database is structured and how

objects are represented in the database.

* Understand key Security Management Server processes and their debugs.
* Understand how GuiDBedit operates.
* Understand how the kernel handles traffic and how to troubleshoot issues with chain modules.
* Understand how to use the two main procedures for debugging the

Firewall kernel and how they differ.

* Recognize User mode prcesses and how to interpret their debugs.
* Discuss how to enable and use core dumps.
* Understand the processes and components used for policy installs and processing packets in Access Control policies.
* Understand how to troubleshoot and debug issues that may occur with App Control and URLF.
* Understand how to debug HTTPS Inspection-related issues.
* Understand how to troubleshoot and debug Content Awareness issues.
* Understand how IPS works and how to manage performance issues.
* Understand how to troubleshoot Anti-Bot and Antivirus.
* Recognize how to troubleshoot and debug Site-to-Site VPN- related issues.
* Understand how to troubleshoot and debug Remote Access VPNs.
* Understand how troubleshoot Mobile Access VPN issues.
* Recognize how to use SecureXL features and commands to enable and disable accelerated traffic.
* Understand how the server hardware and operating system affects

the performance of Security Gateways.

* Understand how to evaluate hardware configurations for optimal performance.