Check Point Threat Prevention Specialist (CTPS) R81_20

Duration: 2 Days   Course Code: CKT_CTPS_R81_20   Delivery Method: Company Event

Overview:

This two-day Specialist-level course is designed for security professionals who want to gain the concepts and skills necessary to deploy and manage Custom Threat Prevention within a Check Point Security environment.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

Security professionals who want to customize IPS and Anti-Bot/Anti-Virus Protections for specific security needs and identify ways to optimize Threat Prevention performance.

Prerequisites:

Learning Path

Training:

• CCSA (required)

• CCSE (recommended)

Prerequisites

Base Knowledge:

• Internet Fundamentals

• Networking Fundamentals

• Networking Security

• System Administration

NIST/NICE

Work Role Categories:

• Implementation & Operation

• Protection & Defense

Testing and Certification

Visit Pearson Vue at vue.com/checkpoint.
Certification Exam#: 156-590
Exam vouchers available at an additional charge – please ask for details.

Follow-on-Courses:

Advanced, self-paced training (coming soon to www.checkpoint.com).

- Threat Emulation

- Threat Extraction

- Zero Phishing

Content:

Module 1: History of Threat Prevention

Lab Tasks

• Verify the Security Environment

• Verify Connectivity Between Systems

Module 2: IPS Protections

Lab Tasks

• Enable and Configure Custom Threat Prevention

• Configure the Inspection Settings

• Update IPS Protections

• Configure General and Specific Protections

• Configure and Test Core Protections

Module 3: Anti-Virus and Anti-Bot Protections

Lab Tasks

• Enable Anti-Bot and Anti-Virus

• Configure Anti-Bot and Anti-Virus

Module 4: Threat Prevention Policy Profiles

Lab Tasks

• Create Custom Threat Prevention Profiles

• Configure the Custom Profiles

• Configure Anti-Bot and Anti-Virus in the Custom Profiles

Module 5: Threat Prevention Policy Layers

Lab Tasks

• Configure Gateway Interface Settings

• Configure Threat Prevention Policy Layers

• Configure Threat Prevention Rules with Custom Profiles

Module 6: Threat Prevention Logs and Traffic Analysis

Lab Tasks

• Modify Threat Prevention Logs and Configure SmartEvent Settings

• Test Threat Prevention Protections

• View Threat Prevention Logs and Events

• Use Web SmartConsole to View Logs and Events.

Module 7: Threat Prevention Exceptions and Exclusions

Lab Tasks

• Use IPS and Threat Prevention Exceptions

• Create an Inspection Settings Exception

• Create a Core Activations Exception

Module 8: Correlated Threat Prevention Views and Reports

Lab Tasks

• Verify SmartEvent Activation

• Generate and Verify Logs for Reporting

• Configure SmartEvent Views and Reports

Module 9: Threat Prevention Updates

Lab Tasks

• Verify Recent Updates

• Configure Update Settings

Module 10: Threat Prevention Performance Optimization

Lab Tasks

• Analyze Threat Prevention Performance

• Create Penalty Box Exceptions and Null Profiles

• Test the Panic Button Protocol

Additional Information:

Please note that courseware is provided in e-kit format for training courses.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK