

CP-CTPS

CHECK POINT THREAT PREVENTION
SPECIALIST R81.20

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
2 Days	Specialist	Check Point / Threat Prevention	ILT/VILT	IGS

INTRODUCTION

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.

AUDIENCE PROFILE

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.

NIST/NICE

Work Role Categories:

- Implementation & Operation
- Protection & Defence

PREREQUISITES

CCSA Required, CCSE recommended.

Base knowledge required:

- Internet Fundamentals
- Networking Fundamentals
- Networking Security
- System Administration

MODULES

Topics

- History of Threat Prevention
- IPS Protections
- Anti-Virus and Anti-Bot Protections
- Threat Prevention Policy Profiles
- Threat Prevention Policy Layers
- Threat Prevention Logs and Traffic Analysis
- Threat Prevention Exceptions and Exclusions
- Correlated Threat Prevention Views and Reports
- Threat Prevention Updates
- Threat Prevention Performance Optimization
- Advanced Threat Prevention Features and Troubleshooting

Lab Exercises:

- Verify the Security Environment
- Verify Connectivity Between Systems
- Enable and Configure Custom Threat Prevention
- Configure the Inspection Settings
- Update IPS Protections
- Configure General and Specific Protections
- Configure and Test Core Protections
- Enable Anti-Bot and Anti-Virus
- Configure Anti-Bot and Anti-Virus

- Create Custom Threat Prevention Profiles
- Configure the Custom Profiles
- Configure Anti-Bot and Anti-Virus in the Custom Profiles
- Configure Gateway Interface Settings
- Configure Threat Prevention Policy Layers
- Configure Threat Prevention Rules with Custom Profiles
- Modify Threat Prevention Logs and Configure SmartEvent Settings
- Test Threat Prevention Protections
- View Threat Prevention Logs and Events

- | | | |
|---|---|---|
| <ul style="list-style-type: none">– Use Web SmartConsole to View Logs and Events.– Use IPS and Threat Prevention Exceptions– Create an Inspection Settings Exception– Create a Core Activations Exception– Verify SmartEvent Activation | <ul style="list-style-type: none">– Generate and Verify Logs for Reporting– Configure SmartEvent Views and Reports– Verify Recent Updates– Configure Update Settings– Analyze Threat Prevention Performance– Create Penalty Box Exceptions and Null Profiles | <ul style="list-style-type: none">– Test the Panic Button Protocol– Add a Custom SNORT Rule– Create and Test a Custom Threat Indicator– Observe Traffic Drops in Real Time– Audit Configuration Changes |
|---|---|---|

ASSOCIATED CERTIFICATIONS & EXAM

This course prepares delegates to write the Check Point Threat Specialist #156-590 exam.