

Checkpoint

Exam 156-727.77

Threat Prevention

Version: Demo

[Total Questions: 10]

Question No : 1

What filters can be used in Check Point ThreatWiki (either via ThreatWiki.checkpoint.com or via ThreatPrevention tab in Dashboard)?

- A. Malware Name, Malware Type
- B. Categories, Risk, Release Date
- C. Risk, Malware Type, Release Date
- D. Categories, Tags, Risk

Answer: D

Question No : 2

When is the default Threat Prevention profile enforced?

- A. At the first Security Policy installation.
- B. Only after SensorNET participation is enabled.
- C. When the profile is assigned to a gateway.
- D. When the administrator installs the profile on Security Gateway.

Answer: D

Question No : 3

A customer does not own Check Point Gateways, but he wants to use Threat Emulation Service to detect SMTP Zero-Day vulnerabilities. What is his option?

- A. Needs to buy a Check Point security gateway.
- B. Purchase TE cloud service.
- C. Use SMTP plug-in on his exchange server.
- D. Needs to install Mail Transfer Agent on his firewall.

Answer: B

Question No : 4

Checkpoint 156-727.77 : Practice Test

What is the name of Check Point collaborative network that delivers real-time dynamic security intelligence to Check Point threat prevention blades?

- A. ThreatSpect
- B. ThreatWiki
- C. ThreatCloud
- D. ThreatEmulator

Answer: C

Question No : 5

Bots and viruses appear as _____ in the reporting blade.

- A. Threats
- B. Incidents
- C. Malware
- D. Infections

Answer: C

Question No : 6

Which of the following statements regarding the threat prevention database is NOT correct?

- A. The Security management server connects to the internet to get Malware Database updates.
- B. By default, updates run on the security gateway every two hours.
- C. The malware database only updates if you have a valid Anti-Bot/ or Anti-Virus contract.
- D. The security gateway contains a local cache of the malware requests.

Answer: A

Question No : 7

IPS is primarily a _____-based engine.

- A. Signature
- B. Difference
- C. Action
- D. Anomaly

Answer: A

Question No : 8

Damage from a bot attack can take place after the bot compromises a machine. Which of the following represents the order by which this process takes place? The bot:

- A. infects a machine, communicates with its command and control handlers, and penetrates the organization.
- B. penetrates the organization, infects a machine, and communicates with its command and control handlers.
- C. communicates with its command and control handlers, infects a machine, and penetrates the organization.
- D. penetrates the organization, communicates with its command and control handlers, and infects a machine.

Answer: B

Question No : 9

IPS can assist in the discovery of unknown buffer overflow attacks without any pre-defined signatures.

- A. False, only the Threat Emulator blade can discover unknown attacks.
- B. True, if Zero-Day vulnerability is enabled.
- C. False, IPS needs predefined signatures for all functions.
- D. True, if Malicious Code Protector is enabled in IPS.

Answer: D

Question No : 10

Check Point Intrusion Prevention System (IPS) is available in two deployment methods, as

Checkpoint 156-727.77 : Practice Test

a blade and also a dedicated appliance. What is the dedicated appliance called?

- A. InterSpect Appliance
- B. IPS-1 Sensor
- C. Smart-1 Appliance
- D. Power-1 Appliance

Answer: B

Thank You For Trying 156-727.77 PDF Demo

To try our 156-727.77 Premium Files visit link below:

<https://examsland.com/latest-exam-questions/156-727.77/>

Start Your 156-727.77 Preparation

Use Coupon **EL25 for extra 25% discount on the purchase of Practice Test Software.**