156-727.77 Q&As

Threat Prevention

Pass CheckPoint 156-727.77 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/156-727-77.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

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.

Correct Answer: D

QUESTION 2

SmartEvent has several components that work together to help track down security threats. What is the function of the Correlation Unit as one of those components in the architecture? The Correlation Unit:

A. connects with the SmartEvent Client when generating reports.

B. analyzes each log entry as it enters a log server, according to the Event Policy; when a threat pattern is identified, an event is forwarded to the SmartEvent Server.

C. collects syslog data from third party devices and saves them to the database.

D. correlates all the identified threats with the consolidation policy.

Correct Answer: B

QUESTION 3

Which of these is a Check Point Firewall attribute?

A. Malicious P2P application protection

B. Buffer overflow prevention

C. Worm injection blocking

D. Granular access control

Correct Answer: D

QUESTION 4

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.

Correct Answer: B

QUESTION 5

What is the name of the Check Point cloud-driven Knowledgebase?

A. ThreatSpect

B. ThreatCloud

C. ThreatWiki

D. ThreatEmulator

Correct Answer: C