CheckPoint 156-730 Exam

Volume: 40 Questions

Question No: 1
Which protocols are supported by the THREAT EMULATION blade?

A. CIFS, FTP, and optional HTIP and SMTP support

B. HTIP(S), SMTP/TLS only

C. HTIP and SMTP only, there is no SSL/TLS security support

D. HTIP(S), SMTP/TLS with optional CIFS

Answer: D

Question No: 2
Which SmartConsole can you use to view Threat Emulation forensics reports?

A. SmartView Monitor

B. SmartView Reporter

C. Smartlog

D. SmartDashboard

Answer: C

Question No: 3
How does Threat Extraction work?

A. Scan and extract files for Command and Control activity.

B. It emulates a document and, if malicious, converts it into a PDF.

C. It extracts active content from a document.

D. It scans the document for malicious code and removes it.

Answer: C

Question No: 4
What kind of approach or approaches will Check Point SandBlast apply to prevent malicious EXEfiles?

A. Machine learning algorithm

B. Signature

C. Exploit

D. Whitelist and Exploit

Answer: C

Question No: 5
You have installed the SandBlast Agent with forensics. An attack has occurred, which triggered the Forensics Blade to collect information. You clicked to open the forensics report but for some reason it is not showing the report as it should. What could be the issue?

A. The attack was based on a macro and the Forensics Blade only supports executables.

B. There is a Microsoft update missing which causes the report not to show as it should.

C. There was no real attack and this is a false positive.

D. Threat Emulation is disabled.

Answer: B

Question No: 6
The file reclassifier is a Threat Emulation component used to perform which function on files in the stream?

A. Count the hits of each file extension, used as part of the reporting mechanism.

B. Used to measure Threat Emulation usage and reporting back to Check Point.

C. Used to rename files extension so they are processed using the correct application based on the file magic.

D. Used to rename files extension so they are processed using the correct application based on the current file extension.

Answer: D

Question No: 7
Which of the following is FALSE about the Sand Blast Agent capabilities?

A. Stop data exfiltration to prevent disclosure of sensitive information, and quarantine infected systems to limit spread of malware.

B. Detect and block command and control communications, even when working remotely.

C. Connect to remote offices via virtual private networking in order to gain secure access to local resources.

D. Get unparalleled visibility into specific endpoint and processes to enable faster recovery postinfection.

Answer: C

Question No: 8
With regard to SandBlast Cloud emulation, which statement is INCORRECT?

A. Sand Blast Cloud licensing offers fair usage caps which customers should never reach.

B. SandBlast Cloud licensing requires a license SKU per gateway.

C. Only new files not seen before are emulated on the cloud and count against fair usage cap.

D. For simplicity, SandBlast Cloud offers a single license SKU per User Center, covering all files sent from all gateways in that User Center.

Answer: D

Question No: 9
Threat Emulation Cloud offers pods to perform emulation, in which geographies are these pods located

A. USA and Germany only

B. Germany, Israel, USA

C. UK, USA, South America

D. Israel, Germany, Russia

Answer: B

Question No: 10
You can restrict a user from downloading an original file if it is getting a malicious verdict from Threat Emulation?

A. True - This is possible through the SmartDashboard Threat extraction settings.

B. False - Due to security concerns, a user will never be able to download a file found to be malicious.

C. True - Under Threat emulation settings you can configure this option.

D. False - Threat Emulation provides a recommendation verdict. The user can download the file even if it is found to be malicious.

Answer: C

Question No: 11
Which deployment modes support Prevent?
1. Inline
2. SPAN port
3. MTA

A. 1 and 3 are correct

B. 1, 2, and 3 are correct

C. 1 and 2 are correct

D. 2 and 3 are correct

Answer: A

Question No: 12
What are the Sand Blast deployment options?
1. Cloud emulation
2. Emulation on the Endpoint itself
3. Local Emulation

4. Remote emulation

A. 1 and 2 are correct

B. 1 and 3 are correct

C. 1, 3, and 4 are correct

D. 2 and 3 are correct

Answer: C

Question No: 13
Regarding a proper Threat Emulation sizing for an environment with 1000 users for web and email traffic which assumptions are correct?
1. 2000 unique files per day within SMTP/S
2. 2500 unique files per day within HTTP/S
3. 7000 unique files per day within SMTP/S
4. 5000 unique files per day within HTTP/s

A. 1 and 2 are correct

B. 1 and 3 are correct

C. 1 and 4 are correct

D. 2 and 3 are correct

Answer: A

Question No: 14
Which command do you use to monitor the current status of the emulation queue?

A. tecli show emulator queue

B. tecli show emulator emulations

C. tecli show emulator queue size

D. tecli show emulation emu