Checkpoint

Exam 156-730

Check Point Accredited Sandblast Administrator

Verson: Demo

[Total Questions: 10]

Question No : 1

What are the deployment methods available with the SandBlast Agent? Choose the BEST answer.

A. Using GPO or SCCM to deploy the deployment agent.
B. Using Configure SandBlast Agent to collaborate with Emulation and Ant-Virus solutions update to upgrade and install the SandBlast Agent.
C. Using both GPO or SCCM for deployment agent and End Point management to push the Agent.
D. Manually installing on every station.

Answer: C

Question No : 2

Select the true statement about Threat Emulation Open Server appliances.

A. Supports custom images without any special requirement.
B. No requirement to enable VT (Hardware Virtualization).
C. Only Cloud emulation service is supported on an open platform.
D. Threat Extraction is not supported on an open platform.

Answer: C

Question No : 3

When enabling Threat Emulation on a standard Check Point gateway, which command allows you to offload emulation to multiple private cloud SandBlast appliances?

A. ted add remote
B. tecli add remote emulator
C. add te remote emulator
D. tecli advanced remote

Answer: D

Question No : 4

Why should you use a Mail Transfer Agent when configuring Prevent/Hold-mode?

1. TE inspection in streaming mode can cause the sending mail server not to send any additional emails until the emulation of the prior email is completed.

2. TE inspection in Mail Transfer Agent mode will accept all valid incoming emails before inspection.

3. It will allow the email to reach the user while at the same time be sent for Dynamic Analysis.

4. There is no Mail Transfer Agent mode for Threat Emulation, only for Anti-Spam.

A. 2 and 4 are correctB. 2 and 3 are correct
B. 1 and 2 are correct
C. All are correct

Answer: C

Question No : 5

What Mail Transfer Agent is used with SandBlast?

A. ExchangeB. Check Point
B. Postfix
C. Sendmail

Answer: C

Question No : 6

What attack vectors are protected by using the SandBlast Agent?

A. Mail, Web, Office 365B. Outside the office, removable media, lateral movement
B. Office 365, Outside of the office, removable media, lateral movement
C. email, Lateral movement, Removable media, encrypted channels

Answer: B

Question No : 7

Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

1. You can assign multiple profiles per gateway.

2. A profile can be assigned to one or more rules.

3. Only one profile per gateway is allowed.

4. A profile can be assigned to only one rule.

A. 1 and 2 are correctB. 1 and 4 are correct
B. 2 and 3 are correct
C. 1, 2, 3 and 4 are correct

Answer: C

Question No : 8

With regard to SandBlast Cloud emulation, which statement is INCORRECT?

A. SandBlast 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

What kind of approach or approaches will Check Point SandBlast apply to prevent malicious EXE-files?

A. Machine learning algorithmB. Signature
B. Exploit
C. Whitelist and Exploit

Answer: C

Question No : 10

At which layer in the Attack Infection Flow can CPU Level Emulation detect a malicious file?

A. The malware binaryB. The Exploit stage
B. The shell code
C. The vulnerability

Answer: B