TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **156-730**

Title : Check Point Accredited Sandblast Administrator

Version : DEMO

1.Which protocols are supported by the THREAT EMULATION blade?
A. CIFS, FTP, and optional HTTP and SMTP support
B. HTTP(S), SMTP/TLS only
C. HTTP and SMTP only, there is no SSL/TLS security support
D. HTTP(S), SMTP/TLS with optional CIFS
Answer: D

2.Which SmartConsole can you use to view Threat Emulation forensics reports?
A. SmartView Monitor
B. SmartView Reporter
C. SmartLog
D. SmartDashboard
Answer: C

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

4.What kind of approach or approaches will Check Point SandBlast apply to prevent malicious EXE-files?
A. Machine learning algorithm
B. Signature
C. Exploit
D. Whitelist and Exploit
Answer: C

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