DUMPSARENA

IBM Certified Associate Administrator - Security QRadar SIEM V7.2.8

Checkpoint 156-730

Version Demo

Total Demo Questions: 5

Total Premium Questions: 40

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

How can CPU Level Emulation detect ROP?

A. Locate a CPU flow buffer with mismatch between called and returned addresses.

B. Increased CPU temperature.

C. Wrong order in the ROP Gadgets Dictionary.

D. It is detected as soon as the evasion code runs and injects the malicious code into a legitimate process.

ANSWER: A

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

How can the SandBlast Agent protect against encrypted archives?

A. The SandBlast Agent cannot protect from an encrypted malware.

B. Since to open the encrypted archive the user must know the password, once opened and the writing to the disk has begun. the SandBlast Agent will immediately scan the file.

C. Password protected archive file is opened via brute force and dictionary attack. Once file is open the SandBlast Agent can scan it and send it to emulation.

D. Only if the administrator has added a special password file and the password that is used for the archive is part of the password list on the file.

ANSWER: D

QUESTION NO: 4

A Threat Extraction license is always bundled with Threat Emulation.

A. False – they can be purchased separately.

B. True – it is part of the NGTX license.

C. True – it is part of the NGTP and EBP license.

D. False – Threat extraction is part of the basic NGFW license.

ANSWER: A

QUESTION NO: 5

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