

DUMPSBOSS.

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://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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

ANSWER: B

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 running the Threat Emulation first time wizard, which of these is NOT an option for file analysis location?

- A. ThreatCloud Emulation Service
- B. tecli advanced remote
- C. Locally on this Threat Emulation Appliance
- D. Other Threat Emulation Appliance

ANSWER: B

QUESTION NO: 4

With regard to SandBlast licensing options, which is INCORRECT?

- A. The NGTP package offers the most complete Threat Prevention offerings
- B. The TETX package can be added on top of NGTP package to create the NGTX package

- B. The TETX package includes both Threat Emulation and Threat Extraction
- C. The NGTX package offers the most complete Threat Prevention offerings

ANSWER: A

QUESTION NO: 5

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