

PaloAltoNetworks.XDR-Engineer.v2026-09-13.q53

□□□□:	XDR-Engineer
□□□□:	Palo Alto Networks XDR Engineer
□□□:	Palo Alto Networks
□□ □□ □□□:	53
□□:	v2026-09-13
# □□ □:	143
# □□ □□□:	530
https://www.krdump.com/PaloAltoNetworks.XDR-Engineer.v2026-09-13.q53.html	

NEW QUESTION: 1

□□□ □□□□ Windows XDR Collector □□□□□ □□ □□□□ OS □□□□□ □ □□□□ □ □□ □□□□ □□□□. □□□ □□□ □□□ □□ □□□□ □□ □□□□□?

- A. □□□ 5MB□□ □□□.
- B. Winlogbeat □□□□□.
- C. Filebeat □□□□□.
- D. □□□ 1MB □□□□□.

Answer: (SHOW ANSWER)

Windows OS □□□□□ □, □□□ □□□ XDR Collector □□ □□□□ □ □ □□ □□ □□ □□□ □ □□□□. Cortex XDR Collector□ □□ □ □□□ □ □□ □□□ □□□ □ □□ □□□□. □□□□ □□ □□(□□□□□ □ □□□)□ □□□□ □□□□ □□□ □ □□ □ □□□□. 5MB □□□ □□□ □□□ □ □□□, □□ □□ Cortex XDR □□□ □ □□ □□□□ □ □ □ □□□□.

NEW QUESTION: 2

□□ □□ □□□ □□□□ □ □□□□ □□ □□□□□ □□□ □□□ □ □□□ □□□ □□□□□, □□ □□□ □□□□ □□□ □ □□□□. □□□ □□□□ □□□□ □□ □ □□ □□□ □ □□□□?

- A. □□ □□ □□ □ □□□□ □□□ □ □□□□.
- B. □□□ □□□ □□□□ □□□□□ □□□ □□ □□□□ □□ □□□ □□□□□ □□ □□ □□ □ □□□□.
- C. □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □ □□□□.
- D. □□ □□ □□ □□ □□□□ □□□□ □□ □□ □□ □□ □□□ □□□□□ □□□ □ □□ □ □□□□.

Answer: D (LEAVE A REPLY)

□ □□□□□ □□ □□ □□ □□□ □□□ □ □□ □□□ □□□ □□□□□.

□□ 1: □□□□ □□□ □ □□□ □□□□□ □□□ □□□□□ □□□ □ □□□□.

□□ 2: □□□□ □□ □□

□□□□□ □□ □□□ □□□ □□□□ □□□ □□□ □□ □□ □□ □□/□□ □□□

□ □□□□ □□ □□□□ □□□, □ □□□□□ □□ □□□ □□ □□(□□□□ □□□

□ □□ □□□ □□□)□ □□□□ □□ □□ □□□ □□□□.

NEW QUESTION: 3

XDR Collector□ □□□□ Windows □ Linux □□□ □□□ □□□ □ □□ □□ □□□□

□□ □□ □□□ □□□ □□□□□?

- A. □□□□
- B. HTTP □□□ □□□
- C. XDR □□□ □□
- D. Winlogbeat

Answer: ([SHOW ANSWER](#))

XDR Collector□ Windows □ Linux □□□ □□□□ Filebeat □□□ □□□□, Cortex

XDR□ □□ □□□□ □□ □□□ □ □□ □□ Filebeat □□□□ □□□□□.

NEW QUESTION: 4

□□ □□ □□□ □□ □, □□ □□□□□ □□ □□□ □□ □□ □□□ □□□□□□□.

□□□ □□ □□□ Windows □□□□□□□ Python □□□□ □□□□ □□ □□□□ □

□□□□□. □□ □□□ □□□ □□□□ □□□?

- A. □□ □□ □□ □□(ABIOCI)
- B. □□ □□ □□(BIOCI)
- C. □□□□
- D. □□ □□(IOCI)

Answer: ([SHOW ANSWER](#))

□ □□ □□□ BIOCI(□□□□ □□ □ □□ □□)□ □□ □□□□ □□ □□ □□□□. □

□□ □□□□□□□ □□ □□□□□□ □□□□□ □□(□: □□□ □□ □□□□

Windows □□□□□ Python□ □□□□ □□)□ □□□□ □□□ □□□□□. BIOCI□ □

□□ □□□□□ □□ □□ □□□□□ □□□ □□ □□□□□□□.

NEW QUESTION: 5

□□ □□□ □□□□ □□□□□?

L_TRIM("a* aapple", "a")

- A. '□□'
- B. "□□"
- C. "□□"
- D. " □□-"

Answer: A ([LEAVE A REPLY](#))

XDR □□□□□ □□ □□□□ □□□ □□□ □□□□□□ □□ □□ □□□ □□□□ □ □□□. □□□ □□□□ □□□ □□□□□. □□□ □□□□□ □□□□□, □□ □ □□ □ □□□ □□□□□. □□□ □□□ □□ □□□ □□□□□□ □□□ □□ □□□?

A. MITRE ATT&CK □□□□ "□□ □□□"□ □□□□ □□□ □□□ □□□□□□.

B. □□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□□.

C. □□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□□□.

D. □□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

Cortex XDR/XSIAM□□ XQL□ □□□□ □□□ □□ □□ □□□ □□□□ □□□ □□□ □ □□ □□ □□□□ □□□□□. □□□ XQL □□ □□□ □□□ □□□ □□□ □□ Cortex□ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□□.

□□ □□□ □□□□□ □□□□ □□ '□□ □□ □□'□□□ □□ □□□ □□□□. □ □ □□□□ XQL □□□□ □□□ □□ □□ □□ □□ Cortex XDR □□ □□ □□□ □□ (□: actor_user_name, target_user_name, host_name)□ □□□□□ □□□ □ □□□□. □ □□□ □□□□ □□□ □□□□□ □□□ □□□ □□ □□□ □□□□ □□□ □□□ □/□□ □□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.

NEW QUESTION: 9

□□ XQL □□□ BIOC(□□ □□ □□ □□) □□□□ □□□ □□ □□□ □□ □□ □□ □□ □□□ □ □□□□?

A. □□□□ = xdr_data

| event_type = ENUM.DEVICE □ action_process_image_name = "***" □□

□□□ action_process_image_command_line = "-e cmd*"

□□□ action_process_image_command_line != "*cmd.exe -a /c*"

B. □□□□ = xdr_data

| event_type = ENUM.PROCESS □ event_type = ENUM.DEVICE □□

action_process_image_name = "***"

□□□ action_process_image_command_line = "-e cmd*"

□□□ action_process_image_command_line != "*cmd.exe -a /c*"

C. □□□□ = xdr_data

| □□ event_type = FILE □ (event_sub_type = FILE_CREATE_NEW □□

event_sub_type = FILE_WRITE □□ event_sub_type = FILE_REMOVE □□

event_sub_type = FILE_RENAME) □ agent_hostname = "hostname"

| action_file_path□ □□□□ □□□□□ action_file_extension□ ("conf", "txt")□ □□□□ □□.

| □□ action_file_name, action_file_path, action_file_type, agent_ip_addresses, agent_hostname, action_file_path

D. □□□□ = xdr_data

* □□ C: dataset = xdr_data | filter event_type = FILE ... □ □□□ □□ □□□□ □□ □□ □□(FILE_CREATE_NEW, FILE_WRITE, FILE_REMOVE, FILE_RENAME) □ □ □□ □□□(event_type = FILE) □ □□□□□□, □□ □□ (/etc/*, /usr/local/share/*, /usr/share/*) □ □□□(conf, txt) □ □□□□ □□□. □ □□□ □ □□□ □□□□ BIOC □□□ □ □□□, □□□ □□ □□ □□□□ □□□□□□ □ □□□ □□□□. Cortex XDR □□ □□□ □□□□□ □□ □□□ □□ □□□□ □□ □ □(□□ □□□□ □□) □ □□□ □□□. □□ □□ BIOC □□□ □□□ □ □□□, Cortex XDR □□ □□□□□ □□ □□□□ □□□(□: □□□□ □□) □□ □□ □□□ (□: □□ □□ □□) □ □□□□ □□ □□ □□□□ □□□□ □□□ □□□□. □□, □□ □□□□ □□□ □□(□: □□ □□ □□, lowercase() □□, fields □) □ □□□□ □□ □ □ □□□□ □□□ □□□□ □□ □ □□□□.

* □□ D: dataset = xdr_data | filter event_type = ENUM.PROCESS ... □ □□□ □□□□ □□□ □□□ □□(action_process_image_name = "***") □ □□□□, □□□□ -e cmd* □ □□□□, *cmd.exe -a /c* □ □□□□ □□□ □□□□ □□□□ □□ □□□(event_type = ENUM.PROCESS) □ □□□□□□□. □ □□□ Cortex XDR □ □□□□□□□ □□□ □ □□ □□ □□□□ □□(□: □□ □□□ □□□ □□□□ □□□□) □ □□□□□ BIOC □□□ □□□□□. □□, □ □□□ BIOC □□ □□□□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□□ □□□ □□ □□ □□□□ □□□ □ □□□□. □□ □□, BIOC □ action_process_image_name = □ □□□□ □□□□□ □□□□□ □□□ □ □ □□□.

"**" □ action_process_image_command_line = "-e cmd*" □ □□□□ □□ □□□□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□ □ □□□□.

□□ □□ (D):

□□ D □ □□□ □□□□□. □ □□□ □□□□ □□ □□(ENUM.PROCESS) □ □□□ □ BIOC □□□□ □□□□ □□□ □□(□□ □□□ □□□ □□□□ □□□□) □ □□□ □ □□ □□□□□. □□ □ □□□ □□ □□□□ □□□□ □□□ □□ □□ □□□□ □ □□ □ □□□, □□□ □□□ □□ □□□□ □□□ □□□□□. □□ □□□ □□□□ Cortex XDR □ BIOC □ □□ □□□□□□□ □□□□□ □□ □□□ □□ □□□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ BIOC □ □□ □□□ □□ □□□ □□ □□□□□. "□□□□ □ □□□(ENUM.PROCESS) □ □□□□□□ XQL □□□ □□ □□□ □□□□ BIOC □ □□□ □□□ □ □□□, □□□ BIOC □□ □□□□ □□□□ □□ □□□ □□□□ □ □□ □□ □□□ □□ □ □□□□." (BIOC □ □□ □□□ □□□ □□□ □□□ □). EDU-260: Cortex XDR □□ □ □□ □□□□□ BIOC □□□ □□ □□□, "□□□□ □□ XQL □□□ BIOC □ □□□□□ □□ □□□□ □□ □□□ □□□ □□ □□□□ □□ □ □ □□□□." (□□ □□□ □□□ □). Palo Alto Networks □□ XDR □□□□ □□□□ □□□ BIOC □□ □□ □ □□ □□□□□ □□□ □□□□ "□□ □□□□□" □ □□ □ □ □□□ □□□□ □□□□.

□□ □□:

Palo Alto Networks Cortex XDR <https://docs-cortex.paloaltonetworks.com/>
EDU-260: Cortex XDR [https://www.paloaltonetworks.com/services/education](https://www.paloaltonetworks.com/services/education/#xdr-)
[/xdr-](https://www.paloaltonetworks.com/services/education/#xdr-)

NEW QUESTION: 10

Cortex XDR `event_type = ENUM.MOUNT` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

- A. `event_type = xdr_data` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT`
- B. `event_type = ENUM.MOUNT` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT`
- C. `event_type = ENUM.MOUNT` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT`
- D. `event_type = ENUM.MOUNT` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT`

Answer: A ([LEAVE A REPLY](#))

Cortex XDR `event_type = ENUM.MOUNT` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

Cortex XDR `event_type = ENUM.MOUNT` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

* `event_type = xdr_data` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

* `event_type = xdr_data` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

* B. `event_type = xdr_data` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

* C. `event_type = xdr_data` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

* D. `event_type = xdr_data` and `event_sub_type = ENUM.MOUNT_DRIVE_MOUNT` are used to detect USB device control events. Which of the following is the correct configuration for the event type and sub-type?

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ □□ □□□□□ □□ □□□ □□ □□□□□. "□□ □□ □ □ □□□□ □□□ □□□□□ □□□ □□□□ □□□□, □□ □□□ □□□ □□□□ -> □□□ □□□□ □□□ □ □□□□." (□□ □□ □□ □□□ □□□ □). EDU-262: Cortex XDR □□ □ □□ □□□□□ □□ □□□ □□□, "□□ □□ □□□□□ □□□□ □□□ □□□ □□ □□□ □□□□□□ □□□ □□□□□ □□□ □□□□ □□□ □ □□□ □." (□□ □□□ □□□ □). Palo Alto Networks □□ XDR □□□□ □□□ □□□□□□ □ □□□□□ □□□ □□□ □□□ "□□ □□ □ □□ □□"□ □□ □□ □□□ □□□ □ □□□□.

□□ □□:

Palo Alto Networks Cortex XDR □□ □□: <https://docs-cortex.paloaltonetworks.com/>
EDU-262: Cortex XDR □□ □ □□ □□ □□ Palo Alto Networks □□ XDR □□□□ □ □□□□: <https://www.paloaltonetworks.com/services/education>
/□□#xdr-□□□□

NEW QUESTION: 11

□□□ □□ □□(MDM) □□□□ □□□ □□ □□□□ Cortex XDR □□□□□ □□□ □, □□ □□□□ □□ □□□ "□□□□□ □□□"□□ □□□□□. □□□ □□□ □□□ □ □□□ □□□□□?

- A. Safari Safeguard □□□ □□ □□□□□ □□ □□□□□ □□ □□□□.
- B. □□□□ □ EDR □□ □□□ □□ URL □□□□ □□ □□□□□ □□□□ □□ □□ □□.
- C. □□□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□□ □□□□.
- D. □□ □□□□ □□ □□□□□ URL □□□ □□□ □□□□□□ □□□□.

Answer: A ([LEAVE A REPLY](#))

□□□ □□□□ Safari Safeguard □□□ □□□□ □□ □□, □□□□□ '□□□□□ □ □□'□□ □□□ □ □□□□. □□ □□□□□ □□ Safari Safeguard□ □□□□□ □ □ □ □□ □□□ □□□ □□□ □□, □□□□□ □□□□□ □□□ □□□□ □□ □□ □ '□□□□□ □□□'□□ '□□□□'□□ □□□□□.

NEW QUESTION: 12

□□□□ □□□□□ □□ □□□ □ □□ □ □□ □□□ □□□ □□□□□? (□ □□□ □□□□□□.)

- A. □□ □□□□□ □□
- B. □□ □□ □□ □□
- C. XQL □□ □□
- D. □□ □□□□□ □□ □□

Answer: ([SHOW ANSWER](#))

Cortex XDR에 대해 옳은 설명은 무엇입니까?

- A. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼입니다.
- B. Cortex XDR은 1000개의 엔드포인트를 *지원하는 통합 보안 플랫폼입니다.
- C. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안, 클라우드 기반의 보안, 클라우드 기반의 보안.
- D. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안 25000개의 엔드포인트를 지원합니다.

Answer: (SHOW ANSWER)

Cortex XDR은 클라우드 기반의 통합 보안 플랫폼입니다. Cortex XDR은 클라우드 기반의 보안, 클라우드 기반의 보안, 클라우드 기반의 보안 (*). Cortex XDR은 클라우드 기반의 보안, 클라우드 기반의 보안, 클라우드 기반의 보안.

NEW QUESTION: 15

Cortex XDR은 클라우드 기반의 통합 보안 플랫폼입니다. Cortex XDR은 클라우드 기반의 보안, 클라우드 기반의 보안, 클라우드 기반의 보안?

- A. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼입니다.
- B. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC).
- C. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC).
- D. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안.

Answer: C (LEAVE A REPLY)

Cortex XDR은 클라우드 기반의 통합 보안 플랫폼입니다. Cortex XDR은 클라우드 기반의 보안, 클라우드 기반의 보안, 클라우드 기반의 보안. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC).

NEW QUESTION: 16

Palo Alto Networks NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC).

- A. NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다.
- B. NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다.
- C. NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다.
- D. NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다.

Answer: (SHOW ANSWER)

Palo Alto Networks NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC). Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC). Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC). Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC).

* (A): NGFW는 Cortex XDR과 통합되어 있으며, 클라우드 기반의 통합 보안 플랫폼입니다. Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC). Cortex XDR은 클라우드 기반의 통합 보안 플랫폼이며, 클라우드 기반의 보안(BIOC).

□□□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□, □□□ □□□□ □□□ □□ □□□ □ □□□□.

* □□ □□□ □ □ □□□?

* B. □□□ □□□(NGFW) □□ □□ □□□ □□□□□. □□ □□□ □□□□ □□ □□ □□ □□□□ □□□ □ □□□ □□□□ □□□ □□□□. □□□ □□ □□□ □ □□□□, □□□ □□□□ □□□□ □□ □□□□ □□ □ □□□□.

* C. □□□ □□□ □□□ □□□□ □□□ □□□□□□. □□□ □□□□ □□□ □□□ □(□: □□□□ □□) □□ □□□□□, □ □□□ □□ □□□□□ □□□□ □□ □ □□ □ □□ □□□□ □□□ □□□□.

* D. NGFW □□□□□□ □□ □□□ □□□□: NGFW □□□□□□ □□ □□□□ □□ □□ □□ Cortex XDR□□ □□ □□ □□□□ □□□ □□□□. □□□□ □□ □□ □□ □□, □□□ □ □□□ □□□ □□ □□ □□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ □□□ □□□(NGFW) □□ □□ □□□ □□□ □□ □□□ □□ □□□□□. "Palo Alto Networks NGFW □□□ □□□□ □□□ □□□□□ XQL □ □(□: dataset = panw_ngfw_logs)□ □□□□ Cortex XDR□ □□ □□□□ □□□ □□□ □□□□." (□□□ □□ □□□□ □□). EDU-260: Cortex XDR □□ □ □□ □□□□□ NGFW □□□ □□□, "□□□ □ NGFW □□□ □□□□ □□□ □□□□ □□ XQL □□ □ □□□□□." (□□ □□□□ □□). Palo Alto Networks □□ XDR □□□□ □□□ □□ □□□□□□□ □□ □□ □□□ □□□ □□□□ "□□□ □□ □ □□"□ □□ □□ □□ □ □□□□ □□□□.

□□ □□:

Palo Alto Networks Cortex XDR □□ □□: <https://docs-cortex.paloaltonetworks.com/>

EDU-260: Cortex XDR □□ □ □□ □□ □□ □□ Palo Alto Networks □□ XDR □□□

□ □□□□□: <https://www.paloaltonetworks.com/services/education>

/□□#xdr-□□□□

XDR-Engineer □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ XDR-Engineer □□! DumpTop □ □□ **XDR-Engineer** □□ □□□ □□□□□□, DumpTop XDR-Engineer □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop XDR-Engineer □□□ □□□□□.

<https://www.dumptop.com/Palo-Alto-Networks/XDR-Engineer-dump.html> (83 Q&As

Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 17

Cortex XDR □□□ □□□□ □□□ □□□□□□ □□ □□ IP □□ □□□□ □□ □□ □□ □□□□ □□□ □□□□□?

A. □□ □□□ □□ □□□ □□□ □□□□□.

B. □□□□ □□ □□□ □□ □□□ □□□ □□□ □□□ □□□□□.

- B. 2400 00, 00 7000 000 00
- C. 2400 00, 00 14000 000 00
- D. 100, 00 240000 000 00

Answer: (SHOW ANSWER)

Cortex XDR 00 0000 00 0000 00000. 0 0000(0000 00 00000 000), 00 0000(0000 000 000 00 000), 000 00 00 00 00 0000 000 0000 0000 00 0 0000 000 0000. 00 000000 0000 0000 00 0000 00 0 0000 000 0000 00 0000 0 0 0 0000 000000. 000 0 0000 000 000 00 00 000, 000 0 000 00 00 000 0000 00 0000.

* 00 00 (B): 00 000000 000 0000 2400 00 00 0 0000 000 00000. 0 00 00 0000 00 0000 0000 00 0000 0 0000. 0 00 00 000 7000, 0 0000 00 0000000 0000 00 0000 0 0 000, 00 00 00 00 000 00000.

* 00 000 0 0 000?

* A. 100, 00 120000 000: 000 000 00 000 Cortex XDR 0 0000 00 000 00 000 0000 0000.

* C. 2400, 00 14000 000 00: 00 2400 00 000 00000, 00 140 00 00000 00 00 00 Cortex XDR 0000 0000 0000.

* D. 100, 00 240000 000: Cortex XDR 000 0000 2400 00 0000 0 00 00 00 00 1000 000 00000.

000 000 00 00:

Cortex XDR 00 000000 000 000 00 000 00 00000. "00 0000 00 000 0000 0 00000 2400 00 0000, 00 70 00 0000 00 000." (0000 00 00 00 00). EDU-262: Cortex XDR 00 0 00 00000 0 00 000 00 000, "00 000000 000 0000 0 000 2400 00 00 00, 00 70 00 0000 00000." (00 00 00 00). Palo Alto Networks 00 XDR 0000 000 00000000 000 0000 000 000 "00 00 0 00 00"0 00 00 000 0000 0000.

00 00:

Palo Alto Networks Cortex XDR 00 00: <https://docs-cortex.paloaltonetworks.com/>

EDU-262: Cortex XDR 00 0 00 00 00 Palo Alto Networks 00 XDR 0000 0

0000: <https://www.paloaltonetworks.com/services/education>

/00#xdr-0000

NEW QUESTION: 19

00 XQL 000 BIOC(00 00 00 00) 0000 000 00 000 00 00 00 00 000 0 0000?

A. dataset = xdr_data| filter event_type = ENUM.DEVICE and action_process_image_name

***"and action_process_image_command_line = "-e cmd*"and
action_process_image_command_line != "*cmd.exe -a /c"

B. dataset = xdr_data| filter event_type = ENUM.PROCESS and event_type =
ENUM.DEVICE and action_process_image_name = "***"and
action_process_image_command_line = "-e cmd*"and
action_process_image_command_line != "*cmd.exe -a /c"

C. dataset = xdr_data| filter event_type = FILE and (event_sub_type =
FILE_CREATE_NEW or event_sub_type = FILE_WRITE or event_sub_type =
FILE_REMOVE or event_sub_type = FILE_RENAME) and agent_hostname = "hostname"|
filter lowercase(action_file_path) in ("/etc/*",
"/usr/local/share/*", "/usr/share/*") □ action_file_extension□ ("conf", "txt")□ □□□□. □
□□ action_file_name, action_file_path, action_file_type, agent_ip_addresses,
agent_hostname, action_file_path□□□.

D. dataset = xdr_data| filter event_type = ENUM.PROCESS and
action_process_image_name
***"and action_process_image_command_line = "-e cmd*"and
action_process_image_command_line != "*cmd.exe -a /c"

Answer: D (LEAVE A REPLY)

BIOC □□□ xdr_data □□□ □□□ □□□ □□□□ □□ □□□ □□□□ □□ □□, □
□ D□ □□□□ □□ BIOC□ □□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□
□ □□□ □ □□□□.

NEW QUESTION: 20

□□ □□□ □□ □□ □□□ □□□□ □□□□?

□□□□ = xdr_data

| □□ agent_hostname, _time, _product

| □□□□ □□□ □□, □□□ □□ □□□ □□ □□□□ □□

| □□ □□=□□(□□□□ = □□□□□)

| □□ endpoint_name, endpoint_status, endpoint_type)□ □□ □□□□ □□

lookup.endpoint_name = agent_hostname

| □□ endpoint_status = ENUM.CONNECTED

| □□ agent_hostname, endpoint_status, latest_time, _product

A. □□□□□□ □□ □□ □□□□

B. □□□□ □□□ □□□ □□□□□ □□

C. □□□ □□□ □□□□□□ □□ □□ □□□□

D. □□□□ □□□ □□□ □□□□□ □□

Answer: A (LEAVE A REPLY)

Cortex XDR□□ □□□□ XQL(XDR □□ □□) □□□ □□□□□ □□□ □□ □□□□
□□□□ □□ □□□□ □□□□ □□□□□. □□□ □□□ □□□□ □□ □□□ □□□
□□□□.

[illegible]

Palo Alto Networks Cortex XDR : Palo Alto Networks  XDR   : <https://www.paloaltonetworks.com/services/education>
/#xdr-

NEW QUESTION: 21

□□□□ □□ □□□ □□ □□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□
□.

IOC□ □□□□ □□□ □□ □□ □□□□□?

- A.** □□ □□□ □□□□□.
- B.** □□ □ □□□ □□ □□ □□□□ □□□□□.
- C.** □□ □□□ □□□□□
- D.** □□ □□□ □□□□□□□□□

Answer: ([SHOW ANSWER](#))

IOC □□□ □□ □□ □□□ □□□□ □□ □□ □□ □□ □□□□ □□□□ □□□ □
 □ □□□ □ □□ □□□□ □□□□□ □□□□□□□□. □□□ □□ □□□ □□ □□□
 □□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □ □□□□.

NEW QUESTION: 22

□□ □□□ □□□□ □□, □□, □□ □□□ □□ □□ □□□□□ □□□□ □□□. □□
□□□□□□ □□□ □□□ □□ □ □□□□□?

- A. PCI DSS** ☐☐
- B. CIS** ☐☐☐☐
- C. MITRE ATT&CK** ☐☐
- D. CVSS** ☐☐☐☐

Answer: C (LEAVE A REPLY)

MITRE ATT&CK□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □.

□□ □□□ ATT&CK□ □□□□ □□□□ □□ □□ □□□ □□□□, □□ □□□□□
□□□, □□ □□ □□□ □□□ □ □□□□.

NEW QUESTION: 23

□□□ □□ □□ □□□ □□□□ □ □□, □□□ VM□□ □□□□□□ □□□ □□□□
□□□□ □□□□□□ □□□ □□□□□ □□□ □□□□□?

- A.** □□□ □□□□ □□□□ □□ □□□ SQL □□
- B.** □□□□□□ □□ □□ □□
- C.** □□□□□□ □□□□ □□□ □□□□ □□□□□□□□.
- D.** □□□□□□□ □□□□ □□ □□

Answer: A (LEAVE A REPLY)

Cortex XDR VM □□ □□□□□□ □□ □□□□ □□□□□□ □□ □
□□□ □□□□□□ □□ □□□ □□□□ □ □□□□□. □□□□ □□□□□ □□□□

- A. 100 10000 100
B. 100 1000 Cortex XDR Analytics1000.
C. 100 100000 100000000.
D. 100 1000 '100 1000'1000.

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 25

1000 10000 1000 1000 10000 1000 10000 1000 1000 1000 1000 1000
100 100000?

- A. 301000 451000
B. 100
C. 51000
D. 1010~2010

Answer: D ([LEAVE A REPLY](#))

Cortex XDR 10000 1000 1000 10000 10000 1000 1000 100 100000.
1000 10000 1000 10000 100 1000 10000, 10000 1000 100 100/100
1000 1010000 2010 1000 10000 1000 1000000.
100 10000 10000 1000000 10000 BIOC100 100 1000 10000000. 100 100
100 1000 100 10000 10000 100 1000000 10000 1000 1000000.

NEW QUESTION: 26

10000 100 100 1000 1000 100 1000 1000 10000 100 1000 10000 10000 100
100 100000. 100 10000 10000 1000000 100 100 1000 10000 100 100
10000 100 100 10000?



- Answer: B (LEAVE A REPLY)**

* □□ □□ (B): □□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□□□. □ □□ □□□ □□□ □□□□ □□□ □□(□□ □□)□ □□ □□□ □ □□□ □□ □□□ □□□□□ □□□□□. □□ □□ □□□□ □□(□: cmd.exe□
cmd /c dir □□)□□ □□ □□□ □□□□ □□□ □□□. □□ □□□ □□ □□□□□, □□□ □□ □□ □□□ □□□□□ □□□□ □□□ □ □□□□ □□ □□□□□ □□ □□□□□.

* A. □□ □□□□ □ □□ BIOC(□□ □□ □□)□ □□ BIOC □□ □□□ □□□□□. □
□ □□: BIOC □□ □□□ □□ □□ BIOC□ □□□ □ □□□, MITRE ATT&CK □□ □
□□ □□□□ □ □ □□□ □□ □□□ Cortex XDR □□(□□□ □□ BIOC□ □□)□ □

□ □□□ □□□ □□□□. BIOC □□□ □□ □□ □□□□□ □□□ □□ BIOC □□□ □ □□□□□.

* C. □□□ □□□ □□ □□□□□ □□ □□□ □□□□ □ □□ □□□ □□□□□.

CortexXDR□□ "□□□□ □□□□ □ □□ □□"□ □□□, □ □□□ □□ □□□□ □□□ □□□□ □□□□. □□□ □□□ □□□□□ □□□ □□□ □□□, □□ □□ □□□□ □□□ □□□□.

* D. □□ □□□□□ □□□ □□□ □□□ □□□ □□ □□ □□□ □□□□□. □□ □ □□□(cmd.exe)□ □□(cmd /c dir)□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□, □□ □□ □□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□. □□□ □□□□□ □□□□□ □□ □□□ □□□□ □□□□, □□ □□ □□□□ □□□□ □□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ □□ □□□ □□ □□□ □□ □□□□□. "□□□□ □□□ □ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□□□." (□□ □□ □□□□ □□). EDU-262: Cortex XDR □ □□ □□ □□□□□ □□ □□□ □□□, "□□□□ □□□ □□□□ □□ □□ □□ □□□ □□ □□□ □□ □□ □□ □□ □□□ □□□□ □□□□□□." (□□ □□□□ □□). Palo Alto Networks □□ XDR □□□□ □□□□□□□ □□ □□ □□□ □□□□ "□□ □□ □□□"□ □□ □□ □□□ □□□□ □□□□.

□□ □□:

Palo Alto Networks Cortex XDR □□ □□: <https://docs-cortex.paloaltonetworks.com/>

EDU-262: Cortex XDR □□ □ □□ □□ □□ Palo Alto Networks □□ XDR □□□□ □

□□□□: <https://www.paloaltonetworks.com/services/education>

/□□#xdr-□□□□

□□□ □□ □□ □□: □□□□ □□□□ □□□□, □□ □□□□(cmd.exe)□ □□

(cmd /c dir)□ □□□ □□□□ □□ □□ □□□□ □□□□□□. □□□□ □□□ □□□ □ □□□□ □□□ □□□ □□□ □□□ □□□ □□ □□□□ □ □□□□.

NEW QUESTION: 27

□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□ □□□□□ DNS □□, □□□□ □□ □ □□□□ □□□ □□ □□□□□ □□□. □□ □□□ □□□□ □□□?

A. □□ □□

B. □□ □□□□

C. XQL □□

D. □□□ □□□ □□□

Answer: (SHOW ANSWER)

XQL □□□ □□□□ □□□□ □□ □□□ □□□ □□□□, □□□ □□□□, □□□ □ □□□, □□□ □□ □□ □□□□□ □□□ □ □□□□. □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□ □□□ □□□□□□□□.

NEW QUESTION: 28

Which of the following is a feature of the Cortex XDR platform? (Select all that apply.)

- A. Real-time threat detection
- B. Automated incident response
- C. Cloud-based architecture, 24/7 monitoring, 4-hour response time
- D. Integration with various security tools

Answer: (SHOW ANSWER)

The Cortex XDR platform is a cloud-based security solution that provides real-time threat detection and automated incident response. It integrates with various security tools and offers 24/7 monitoring and a 4-hour response time. The platform is designed to protect organizations from a wide range of threats, including malware, ransomware, and data breaches.

The Cortex XDR platform is a cloud-based security solution that provides real-time threat detection and automated incident response. It integrates with various security tools and offers 24/7 monitoring and a 4-hour response time. The platform is designed to protect organizations from a wide range of threats, including malware, ransomware, and data breaches.

NEW QUESTION: 29

Which of the following is a feature of the Cortex XDR platform? (Select all that apply.)

- A. Real-time threat detection
- B. Automated incident response
- C. Cloud-based architecture, 24/7 monitoring, 4-hour response time
- D. Integration with various security tools

Answer: B (LEAVE A REPLY)

Live Terminal is a feature of the Cortex XDR platform that allows security analysts to interact with endpoints in real-time. It provides a command-line interface for running commands and executing scripts on the endpoints. This feature is used for investigating incidents and performing remediation actions.

NEW QUESTION: 30

XDR is a type of security solution that provides real-time threat detection and automated incident response. It integrates with various security tools and offers 24/7 monitoring and a 4-hour response time. The platform is designed to protect organizations from a wide range of threats, including malware, ransomware, and data breaches.

The Cortex XDR platform is a cloud-based security solution that provides real-time threat detection and automated incident response. It integrates with various security tools and offers 24/7 monitoring and a 4-hour response time. The platform is designed to protect organizations from a wide range of threats, including malware, ransomware, and data breaches.

□□□□(HA) □□□□ □□□ VM□ □□□ □, □□□ VM□ FQDN□ □□□ □ XDR □ □□□ □□ □□ □ □□ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□□□□ □□□ □□□□ □□ □□ □□□ □□□□□?

- A. □□ □□□ VM□ □□ SSL □□□ □ □□ □□□□ □□ □□□ □□ □□ IP □□□ □□□□□.
- B. □□□ SSL □□ □□□□ □□ □□□□□ □□ □□□□ □□□□□.
- C. □□ □□□□ □□□□ □□ □□□□□ SSL □□□ □□□□□.
- D. □□□ VM □□□□ □□□□ □□ □□□□ □□□□□ □□ □□□ □□□□ □□ □ □□□□.

Answer: B ([LEAVE A REPLY](#))

Cortex XDR□ □□□ VM HA □□□□ □□□□□□ □□ □□□□ FQDN□ □□□□, □ □□ □ □□ CA □□ □□□□ □□□□ □□ □□□ VM□ □□□□□□ □□□□□. □ □ □□ □□□□ □□ □□□ □□□□ □□□, HA□ □□□ □□ □□□□ □□□□□.

NEW QUESTION: 33

□□ □□ □□, Windows Cortex XDR □□□□ □□ □□□□ □□ □□ □□□□ □□□□ □ RDP □□□□ □□□□ □□ □□□ □□□□□□□□. □□ □□□□ □□ □□□ □□□ □□.

- □□ □□□□ Cortex XDR □□□□□□ □□□□□□ □□ □□□□.
- □□ □□□□□□ RDP□ □□□□□ □□ □□□ □□ □□□ □□□ □□□ □□□□.
- □□□□ □□□ □□□□ □□□□□ □□□ □□□ □□□□□.
- □□□ □□ □□ □□ □□□ □□□□□.
- □□ □□□ □□ □□ □□□□ RDP□ □□□□□ □□□□ □□□ □□□□□□□□.
- □□ □□□□ □□□□ □□□□□□.
- □□□□ □□□ □□□□ □□ □□□ □□ □□□□□□ □□□□□□.
- □□□□ □□□□ □□□□ □□ □□□ □□ □□□□□□ □□□□□□.

RDP □□□□ □□□□ □□ □□ □□□ □□□ □□□□□?

- A. □□□□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.
- B. □□ □□□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□□□.
- C. □□□ □□□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□□.
- D. □□ □□□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□□□.

Answer: ([SHOW ANSWER](#)**)**

□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□, □□ □□□ □□ □□ □□□ RDP □□□ □□□□□ □□□□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□.

Cortex XDR은 모든 엔드포인트와 클라우드 서비스에서 발생하는 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. (예: IP 주소, 파일 해시, URL 등)의 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다.

Cortex XDR은 모든 엔드포인트와 클라우드 서비스에서 발생하는 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. (예: IP 주소, 파일 해시, URL 등)의 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다.

NEW QUESTION: 34

다음 중 Cortex XDR의 주요 기능은 무엇입니까?

- A. 100%, 모든 12개월 동안 모든 이벤트를 저장합니다.
- B. 24시간 동안, 모든 7일 동안 모든 이벤트를 저장합니다.
- C. 24시간 동안, 모든 14일 동안 모든 이벤트를 저장합니다.
- D. 100%, 모든 24개월 동안 모든 이벤트를 저장합니다.

Answer: B ([LEAVE A REPLY](#))

Cortex XDR/XSIAM은 모든 엔드포인트와 클라우드 서비스에서 발생하는 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. (CU)은 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. 모든 CU은 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. Palo Alto Networks은 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다.

다음 중 Cortex XDR의 주요 기능은 무엇입니까? XQL은 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. 모든 "XQL"은 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다.

다음 중 Cortex XDR의 주요 기능은 무엇입니까? 모든 CU은 모든 24시간 동안 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. 모든 CU은 모든 24시간 동안 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. 모든 CU은 모든 24시간 동안 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. 모든 CU은 모든 24시간 동안 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다.

NEW QUESTION: 35

다음 중 Cortex XDR의 주요 기능은 무엇입니까?

- A. 모든 이벤트를 저장합니다.
- B. MAC 주소
- C. IP 주소
- D. 모든 이벤트를 저장합니다.

Answer: C ([LEAVE A REPLY](#))

다음 중 Cortex XDR의 주요 기능은 무엇입니까? IP 주소는 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다. 모든 IP 주소는 모든 이벤트를 수집하고 분석하여 위협을 탐지하고 대응합니다.

NEW QUESTION: 36

30□ □□ □□ □□□ □□□ □□□ □□ □□ □□□ Cortex XDR□ □□□□□
 □. □ □□□□□ ITDR(Identity Threat Detection and Response) □□ □□□ □□□□ □
 □□, Cortex □□ □□ □□□□ □□□□ ID □□□ □□□□□□□. □□□ □□ □□□
 □□□ ID □ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□□ □□□□□, □□ □
 □□ □□□, □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□□□
 □?

- A.** XDR □□□□ □□□□ ID □□□ □□□ □□□ □□ □□□□.
- B.** □□□□ ID □□ □□□□ □□ □ □□□□ □□□□□.
- C.** □□□□ ID □□□ □ □□ □□ □□□□ □□□□□□ □□□.
- D.** ITDR □□ □□□ □□□□ ID □□□ □□□□ □□□□.

Answer: A (LEAVE A REPLY)

Palo Alto Networks ID 000 0000 000 000 000 0000 00 0 00 0
0 000 00000. 0000 ID 00(CIE) Cortex XDR/XSIAM 0000 000, 00
00 000 000000 000000 000000 000000 0 0000 00 0000 00
0 0000 000 0000.

Cortex ☐☐ ☐☐ ☐☐ ☐☐ ☐ Cloud Identity Engine ☐☐☐☐ ☐☐☐☐ CIE
☐☐☐ ☐☐ ☐ Cortex XDR ☐☐☐ ☐☐☐ ☐ ☐, ☐☐ ☐☐ ☐☐ ☐
☐☐☐. ☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐ XDR ☐☐ ☐☐ ☐
☐☐.

NEW QUESTION: 37

☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐☐☐☐

☐☐, ☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐ ☐☐☐.



□□□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□ □□ □□ □
 □□ □ □ □□□ □□□ □□□□ □□□ □□□□□ □□□. □□□□□ □ □□ □□
 □ □□□□ □□ □□□ □□ XQL □□□ □□□□□□.

$$\square\square\square\square = \square\square$$

| ☐: alert name, description, alert source, severity, original tags, alert id, incident id

| ☐ ☐ alert name

| ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

[illegible]

(filter alert name =)

- Answer: ([SHOW ANSWER](#))**

[illegible]

```
'= $x_axis.value' □ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□ □□ □  
□ □□□ □□□□ □□□□ □□□□□ □□□.
```

* A. \$y_axis.value: □ □□□ y□ □□ □□□□, □□□□□ □□□□ □□ □(□: □□ □ □)□ □□□□, □□□ □□ □□□ □□□□ □□□□.

```
* D. $y_axis.name: ☐ ☐ ☐ XQL ☐ ☐ ☐ ☐, yaxis alert_name☐ ☐ ☐ ☐ ☐
☐ ☐ ☐ ☐ ☐.
```

□ □ □ □ :

EDU-262: Cortex XDR □□ □ □□ □□ □□

□□□□□□□□ □□ XDR □□□□ □□□□□:
<https://www.paloaltonetworks.com/services/education>
/□□#xdr-□□□□

NEW QUESTION: 38

□□ □□□□ □□□ □□□□ □□□□, □□ □□□ □□□ □□ □□□□□□□□ □□□
□□□□ □□□ □□□ □ □□ □□ □□□□□□ □□□ □□□□.



- A. □□ □□□□□
- B. □□□□ □□□□
- C. □ □□ □□ □□□□□
- D. □ □□ □□ □□ □□□□□.

Answer: (SHOW ANSWER)

□□□□ □□□□ □□□□□, □□□ □□□□ □□□□□ □ □ □□□ □□□ □ □□
□□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□ Cortex XDR □□□□ □□□
□ □□□ □□□□□. Cortex XDR□□ □□ □□ □□ □□□ □□□□ □□□□□□□
□□ □□□ □□□□ □□□ □□□□□. □□□ □□□ □□□ □□ □□□□□□□(□□□
□□□□ □□□□ □□ □□□ □□ □ □ □□ □□ □□)□ □□, □□ □□□
WildFire(Palo Alto Networks□ □□□□ □□ □□ □□ □□□)□□ □□□ □□□□□ □
□□ □□ □□□□□ □□□ □□□ □□□ □□□□ □□□□.

* □□ □□ (B): □□□□□ Cortex XDR□ □□□ □□□□ □□□ □□□ □□□□ □□
□□□ □□□ □□□ □□ □□□□□□□ □□□ □ □ □□ □□ □□□ □□□□□ □
□□□ □□□□. □□□□□□□ □□□ □□□□ Cortex XDR □□□□□ □□ □□□□
(□□□□ □□ □□) □□□ □□ WildFire□ □□□ □, □□□ □□ □□□ □□□ □□□

□□. □□□□□□□ □□ □□□ □□□ □□□ □□ □□ □□□□ □□□□ □□ B□
□□□□□.

* □□ □□□ □ □ □□□?

* A. □□ □□□□□: □□ □□ □□□□□□□ □□ □□□ □□□ □□□ □□□ □ □
□□ □□ □□□ □□□□□ □□□ □□□□ □□□□, □□ □□ □□□□□ □□□□□
□□□□.

* C. 1□□ □□ □□□□□: Cortex XDR□□ □□□ 1□□ □□ □□□□□ □□ □□□
□□□□. □□□ □□□ □□ □□□ □□□ WildFire□ □□ □□ □□ □□□ □□ □□
□□□.

* D. □ □□ □□ □□ □□□□□: Cortex XDR□□ □ □□ □□ □□ □□□ □□□□ □
□□□□ □□□□. □□□ □□ □ □□ □□□ □□ □□□□□ □□□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□ □□□ □□□ □□□ □□ □□□ □□ □□□□□. "□□□□□
□ □ □□ □□ □□□ WildFire□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□
□□□ □□□□□□□□□□ □□□□□." (□□□ □□□ □□ □□□□ □□). EDU-260:
Cortex XDR □□ □ □□ □□□□□ □□□ □□□□ □□□, "□□ □□□ □□□ □□□
□□□ □□□ □□□□ □□ □ □ □□ □□ □□□ □□□□□."□□ □□□□□(□□ □
□□ □□□ □□).

Palo Alto Networks □□ XDR □□□□ □□□□□□□ □□□□ □□□ □□□ □□□□
"Cortex XDR □□□□ □□"□ □□ □□ □□□ □□□□ □□□□.

□□ □□:

Palo Alto Networks Cortex XDR □□ □□: <https://docs-cortex.paloaltonetworks.com/>

EDU-260: Cortex XDR □□ □ □□ □□ □□ □□ Palo Alto Networks □□ XDR □□□□

□ □□□□□: <https://www.paloaltonetworks.com/services/education>

/□□#xdr-□□□□

□□□ □□ □□ □□: □□□□ □□□□ □□□□□ □□ □□□ □□□ □□□□ □□
□□□□. □□□□ □□□ □□□□ □□(□: □□ □□ □□, □□ □□ □□ □□ □□)□
□□□ □□□ □□□ □□□ □□ □□□ □□□ □□ □ □□□□.

NEW QUESTION: 39

Cortex XDR □□□□□ □□□ □□□□□ □□□ □□□ □ □□ □□□□□□ □□□ □
□□□□ □□□ □□□ □□□□□. □□□ □□□ □□□ □□□□ □□ □□ □ □□□
□□□ □□ □ □□□□? (□ □□ □□□□□□.)

A. □□ □□ □□

B. □□□□□ □□□□□ □□ XQL □□

C. □□ □□□□□ □□□

D. □□ □□

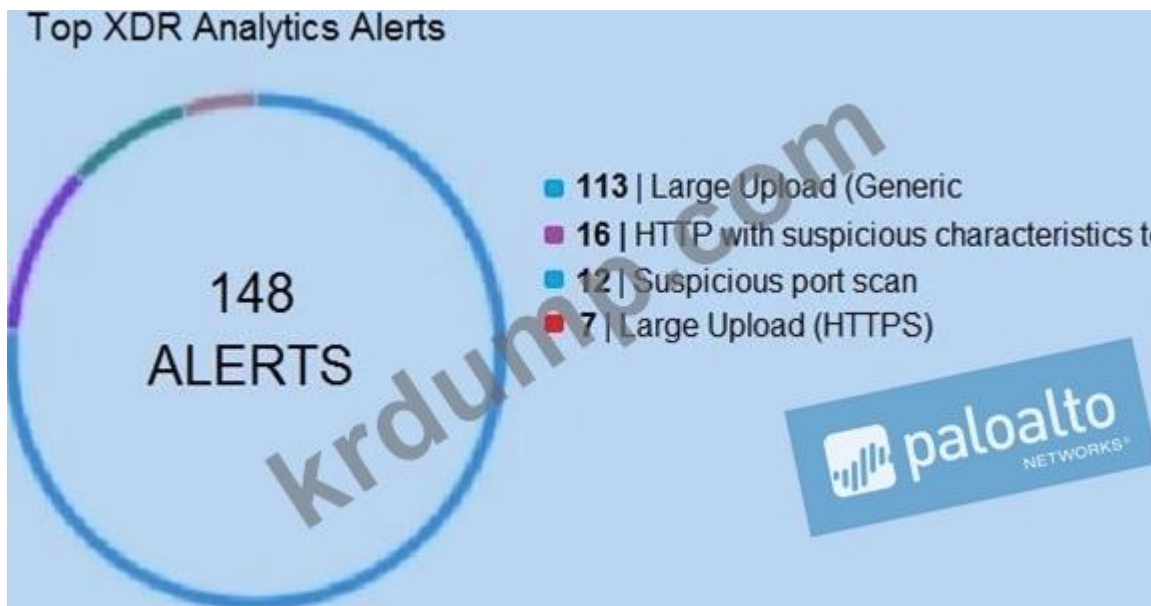
Answer: ([SHOW ANSWER](#))

□□ □□□□□ □□□: □ □□□□ Cortex XDR □□□□ □□□□ □□□ □□□□ □
□ □□□□□. □□□□□ □□□ '□□□□□ □□□'□□ □□□□ □□ □□□ □□ □

Which of the following is a valid Cortex XQL query? (Select all that apply.)
 A. select * from alerts where severity = 'High'
 B. select * from alerts where severity = 'High' and alert_name = 'Malware Detected'
 C. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network'
 D. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network' and alert_id = 1234567890

NEW QUESTION: 40

Which of the following is a valid Cortex XQL query? (Select all that apply.)
 A. select * from alerts where severity = 'High'
 B. select * from alerts where severity = 'High' and alert_name = 'Malware Detected'
 C. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network'
 D. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network' and alert_id = 1234567890



Which of the following is a valid Cortex XQL query? (Select all that apply.)
 A. select * from alerts where severity = 'High'
 B. select * from alerts where severity = 'High' and alert_name = 'Malware Detected'
 C. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network'
 D. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network' and alert_id = 1234567890

Which of the following is a valid Cortex XQL query? (Select all that apply.)

A. select * from alerts where severity = 'High'

B. select * from alerts where severity = 'High' and alert_name = 'Malware Detected'

C. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network'

D. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network' and alert_id = 1234567890

Which of the following is a valid Cortex XQL query? (Select all that apply.)
 A. select * from alerts where severity = 'High'
 B. select * from alerts where severity = 'High' and alert_name = 'Malware Detected'
 C. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network'
 D. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network' and alert_id = 1234567890

A. \$y_axis.value

B. \$x_axis.value

C. \$x_axis.name

D. \$y_axis.name

Answer: (SHOW ANSWER)

Which of the following is a valid Cortex XQL query? (Select all that apply.)
 A. select * from alerts where severity = 'High'
 B. select * from alerts where severity = 'High' and alert_name = 'Malware Detected'
 C. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network'
 D. select * from alerts where severity = 'High' and alert_name = 'Malware Detected' and alert_source = 'Network' and alert_id = 1234567890

□ □□ □□ □□□ □□□ □□ □□□□ □□□ □□□ x□ □□ □□□□ alert_name
□ □□□□ □□□□□ □□□.

NEW QUESTION: 41

□□ □□ 30□ □□ □□ □□□ □□□ □□ □□ □□□ Cortex XDR□ □□□□□□.
□ □□□□□ ID □□ □□ □ □□(ITDR) □□ □□□ □□□□ □□□, Cortex □□ □□
□□□□ □□□□ ID □□□□ □□□□□□□□. □□□□ □□□□ □□□□ ID □ □□
□□ □□□ □□□ □ □□□ □□□ □□□□□ □□□ □□□ □□ □□□ □□□, □□
□□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□□□□?

- A. XDR □□□□ □□□□ ID □□□□ □□□□ □□□ □□ □□□□.
- B. □□□□ ID □□ □□□□□□ □□ □ □□□□ □□□□□.
- C. □□□□ ID □□□□ □ □□ □□ □□□□ □□□□□□ □□□.
- D. ITDR □□ □□□ □□□□ ID □□□□ □□□□ □□□□.

Answer: A (LEAVE A REPLY)

Cortex XDR□ ID □□ □□ □ □□(ITDR) □□ □□□ □□□□ ID □□□□ □□□□ ID □
□ □□ □□ □□□ □□□□□. □□□□ ID □□□□ ID □□□(□: Active Directory, Okta)
□□□□ □□□, □□ □ □□□ □□□ □□□□□□. □□□□ ID □□□□ □□ □□□ □□
□□□□ ID □□□□ □□□□□ Cortex XDR □□□□ □□□ □□□□□ □□□□ □□
□□□□ □□□.

* □□ □□ (A): □ □□□ XDR □□□□ □□□□ ID □□□□ □□□□ □□□ □□ □□ □
□□ □□□□ □□□ □□□□. Cortex XDR □□□□ □□□□ □□□□(□: □□, □□),
□□□□ ID □□□□ □□ □□□ □□ □□□□ □□□□ □□□□□ □□□□□ □□□.
□□ □□□□ □□□□□ □□ □□□ ID □□□□□ □□ □□(□: □□)□ □□□□ ID □
□□□□ □□□□ □□, □□□□ □□ □□□□ □□ □□□, □□ □□ □□□ □□□ □□
□□ □□□ □□□ □□□ □ □□□□.

* □□ □□□ □ □ □□□?

* B. □□□□ ID □□ □□□□□□ □□ □ □□□□ □□□□□. □□□□ □□□□ ID □□
□ □□□□□□□ □□□□ □□□□ □□ □ □□□ □□□ □□□ □□□□□.
□ □□□ □□ □□ □□□□ □□□ □□□, □□□ □□□ □□□ □□□□□ □□ □□
□□□□.

* C. □□□□ ID □□□□ □□ □□□ □□□□ □□□□□ □□□. □□□□ ID □□□□ □
□ □□□□ □□□□ □□□ □□□□. □□□□ □□□ □□□□ □□□□□ □□□□ □
□, □□ □□□□ □ □□ □□□□□.

* D. ITDR □□ □□□ □□□□ ID □□□□ □□□□ □□□□. ITDR □□ □□□ □□□□
ID □□□□ □□ □□□□□ □□□□□□□ □□□□ □□□ □□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ □□□□ ID □□ □□□ □□ □□□ □□ □□□□□. "□□
□, □□ □ □□□ □□□ □□□ □□□□ □□□□ □□ □□□□ ID □□□ Cortex XDR
□□□□ □□□ □□□ □□□□□ □□□." (□□□□ ID □□ □□□□ □□). EDU-260:

Cortex XDR □□ □ □□ □□□ ITDR□ ID □□□ □□□, "□□□ ID □□□□ □□□□ □□□□ □□□□ ID □□ □□ □□□ □□□ □□ □□□□"□ □□□□ □□□□(□□ □□ □□). Palo Alto Networks □□ XDR □□□□ □□□ □□ □□□□ □□□□ ID □□ □□□ □□□□ "□□□□ □□ □ □□"□ □□ □□ □□□ □□□□ □□□□.

Palo Alto Networks Cortex XDR ☐☐ ☐☐: <https://docs-cortex.paloaltonetworks.com/>
EDU-260: Cortex XDR ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ Palo Alto Networks ☐☐ XDR ☐☐
☐ ☐☐☐☐: <https://www.paloaltonetworks.com/services/education>
[/input type="checkbox"/>input type="checkbox"/>#xdr-input type="checkbox"/>input type="checkbox"/>input type="checkbox"/>](#)

Cortex XDR □□□ □□□□ □□□ □□□□□□ □□ □□ IP □□ □□□□ □□ □□
 □□ □□□□ □□□□ □□□ □□□□□?

NEW QUESTION: 43

* □□ □□ (C): □□□□ □□□□□ Microsoft Azure□ □□ □□□□ □□□□□ □□□ □□□□. □ □□□ □□ Cortex XDR□ □□□ □□□□, □□□□ □□□ □ □□□ □□ Azure □□□ □□ □□□□□□ □□□ □□ □□ □ □□□□ □□□□□ □□□□ □ □□□□. □□□□ API □□ □□(□: Azure □□□ □□ □□)□ □□ Azure□ □□□□ □□□□ □□□□□ □□□□ □□ □□□□ Cortex XDR□ □□□□□□.

* □□ □□□ □ □ □□□?

* A. Azure Network Watcher: Azure Network Watcher □ □□□□ □□□ □□□□□□ □
 □□□ Microsoft Azure □□□□□□ □□ □□□ □□□ □□ Cortex XDR□ □□ □□□
 □ □□□ □□□□.

* B. □□□□ ID □□: □□□□ ID □□□ ID □□□(□: Azure AD)□ □□□□ □□□ □
□□ □□□□ □□□□□ ID □□ □□ □□□ □□□□, VM□□ □□□□□ □□ □□ □
□ □□□□ □□□□□ □□□□.

* D. Microsoft 365: Cortex XDR ☐ Microsoft 365 ☐☐☐ ☐☐☐ ☐☐☐☐☐☐
(☐: Exchange ☐☐ Teams) ☐☐☐ ☐☐ Azure ☐☐ ☐☐☐☐☐☐☐
☐☐.

[illegible]

Cortex XDR □□ □□□□□ □□□□ □□□ □□ □□□□□. "□□□□ □ □□□□ Microsoft Azure□ □□□□ □□ □□□□ □□□□ □□□□ □□ □ □□□ □□□□ □□□□ □□ □□□ □□□□□□." (□□□□ □□□□ □□ □□□ □□□ □). EDU-260: Cortex XDR □□ □ □□ □□□□□ □□□□ □□□ □□□ □□ □, "□□□□ □□□□□ Azure□ □□□□ □□ □□□□□□ □□□□□□ □□□□ □ □□□□□." (□□ □□□ □□□ □). Palo Alto Networks □□ XDR □□□□ □□□ □□ □□□□□□□ "□□□□ □□ □ □□"□ □□ □□ □□□ □□□□ □□□□, □□□□ □□ □□ □□ □□□ □□□□ □□□□.

□ □ □ □ :

Palo Alto Networks Cortex XDR  : <https://docs-cortex.paloaltonetworks.com/>

EDU-260: Cortex XDR ☐☐ ☐ ☐☐ ☐☐ ☐☐ Palo Alto Networks ☐☐ XDR ☐☐☐

□ □ □ □ □ □: <https://www.paloaltonetworks.com/services/education>

/□□#xdr-□□□□

NEW QUESTION: 44

□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □□□. □□ □□□ □□□ □□ □
□□□□□□ □□□□ □□□□ □□□□ □□□□□□□. □□ □□□□ □□□□ □□
□ □□ □ □□ □□□ □□□□□? (□ □□□ □□□□□□.)

[□□□ □□: □□ □□ □□□ □□ □□ □□ □□(BIOC) □□□ □□□□□□ □□□ □
□□ □□ □□ □□]

A.

B. XDR □□ □□ □□□(BIOC) □□□ □□ □□ □□□ □□□□□.

C. XDR □□□□ □□□ □□ □□ □□□ □□□□□.

D. □□ □□ □□(BIOC) □□ □□

Answer: A,D (LEAVE A REPLY)

□□□ □□ □□ □□(□□ □□□ □□ □□□ BIOC □□□ □□ □□□□□□ □□□ □
□□□ □□)□□ □□ □□□□ □□□ □□□ □, □□□ □□□ □□□□ □ □□ □□ □
□□ □□□□.

Cortex XDR□□□ □□□ □□ □□ □□□□□□ □□ □□□ □□□ □ □□□□. □□
□□□ □□□□ □□ □□(□: □□ □□□ □□□□□ □□, □□ □□ □□ □□□)□ □
□□□ □□ □□□ □□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□□ □□□
□ □□□□.

□ □□□ □□□□ □□ □□□ □□□ □□ BIOC □□ □□□ □□□□ □□□□□ BIOC
□□ □□□ □□□ □ □□□□. BIOC □□ □□ □□ □□□ □□ □□□□(□: □□ □□
□ □□□□ □□ □□ □□ □□□□ □□ AND NOT □□ □□) □□ □□ □□□ □□□
□□□ □□□□ □□□ □□□ □ □□□□.

NEW QUESTION: 45

□□ □□□□ □□□□ □□ □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□□□
□. Cortex XDR □□□□□ □□ □□ □□□□ □□ □□□□ □□ □□ "□□ □□" □□
□□ □□□□ □□□□. □□□□□ □□□□□ □□□ □□ □ □□□□?

A. □□□ □□□□ □□ -> □□□

B. □□□□ = xdr_data | □□ event_type = ENUM.MOUNT □ event_sub_type =
ENUM.MOUNT_DRIVE_MOUNT

C. □□□ □□□□ □□□□□ □□ □□□ □□□□□.

D. □□ □□ = □□ □□

Answer: C (LEAVE A REPLY)

□□ □□ □□□□ □□ □□□□ □□ □□ □□ □□□□ □□□□ □□, Cortex XDR□
□□ □□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□
□□□ □□□□ □□□□ □□□□.

□□□ □□□ □□□ □□□□□ □□□□□ □□□ □□ □□ □□□□/□□ □□□ □□
□□□ □□ □□ □□ □□□ □□□□□.

NEW QUESTION: 46

Cortex XDR □□□□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□
□ Windows □□□□□ □□ □□□ □□ □ □□□□ □□□ □□□□□?

A. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" □□

B. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" □□□ □□

C. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" -s stop

D. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" occp

Answer: B (LEAVE A REPLY)

□□□□□□□ □□ □□ □□ □□ □□□□□ □□□ □□□ □□□ □ □□□□ □□
cytool CLI □□□□□ □□□□ □□ □□□□ □□□□□ □□□□□.

* C. □□□□(Filebeat) □□□□□. XDR Collector□ □□ □□ □□□ □□ Filebeat□ □□□□. OS □□□□□□ □□ □□ □□□ □□□□ □□ □, □□ □□□ □□□ □□ □□ □□□□ □□□□. (□□ □□□ □□□□□ □□□□ □□ □□□□.)

* D. □□□ 1MB □□□ □□: Cortex XDR□□ □□ □□□□ □□ □□ □□ □□□ □□ □□ □□□ 1MB □□□□□ □□ □□□ □□□□ □□ □□ □□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ □□ □□ □□□ □□ □□□ □□ □□□□□. "XDR □□□ □ OS □□□□□□ □□ □□ □ □□□ □ □□ □□ □□□ □□□□ □□ 5MB□□ □ □□ □□ □□□□ □□□□□." (XDR □□□ □□ □□ □□□□ □□). EDU-260: Cortex XDR □□ □ □□ □□□□□ □□ □□ □□□ □□□, "5MB□ □□□□ □□ □□□□ □□□□ □□□, □□ □□ □□□ □□□□ OS □□□□□ □ □□ □□□□ □□□□ □□." (□□ □□□□ □□).

Palo Alto Networks □□ XDR □□□□ □□□ □□ □□□□□ □□ □□ □□□ □□□ □ "□□ □□ □ □□ □□"□ □□ □□ □□□ □□□□ □□□□.

□□ □□:

Palo Alto Networks Cortex XDR □□ □□: <https://docs-cortex.paloaltonetworks.com/>

EDU-260: Cortex XDR □□ □ □□ □□ □□ □□ Palo Alto Networks □□ XDR □□□□

□ □□□□□: <https://www.paloaltonetworks.com/services/education>

/□□#xdr-□□□□

NEW QUESTION: 48

□□ □ □□ □□□ □□□□ □□□□ □□□ □□□□□ □□□□□□ □□□ □□ □□ □ □□□□□ □ □□□ □□□□□ □□□□ □□□ □□□□□?

A. □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□ □ □□□, □□□□ □ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□□□.

B. □□ □□□ □□□ □□□□ □□□□ □□□□ □□, □□□□ □□□□□ □□ □□ □□ □□□□□□ □□□ □□□□ □□□□ □□□□□ □ □□□□.

C. □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□ □□ □□□□ □□□ □□□ □ □□□, □□□□ □□□□□ □□□ □□□□□ □□□□□ XQL □□ □□□ □□ □ □□ □□□ □□□□□□.

D. □□ □□□ □□ □□□□ □□□□□ □□□ □ □□□, □□□□ □□□□□ □□ □ □□ □/□□ □□□□□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

Cortex XDR□□ □□ □□□ □□□□ □□□□□ □□□□□ □□ □□□□ □□□□ □ □□□□ □□ □□□□□. □□ □□□ □□□□ □□□□ □□ □□□ □ □□ □□ □(□: □□ □□, □□□□ □□ □□ □□)□ □□□□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□□ □□□□ □□□ □□□ □ □□□□. □□ □□□□ □□□□□ □□ □□ □□ □□ □□(□:

□□ □□ □□ □□□ □□□□ □□ □□, □□ □□□□□ □□□□□ XQL(XDR □□ □□) □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□□ □□□ □□ □ □□ □□.

* □□ □□ (C): □□ C□ □□□ □□□ □□□□ □□□□□. □□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□ □□□□ □□□ □□□ □ □□□□ □□ □□□ □□ □□(□: □□ □□□ □□)□ □□□ □ □□□□. □□□□ □□□□□ □□□ □□□□□ □□□□□ XQL □□ □□□ □□ □□□ □□□ □□□□□ □□□□ □□□□□□ □□ □□ □□□□ □□□□□ □□□ □□□ □□□ □ □□□ □□□.

* □□ □□□ □ □□□?

* A. □□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □ □□□ □□ □□, □□□□ □□□□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□. □□ □□□ □□□□□. □□□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□□, □□ □□ □□ □□□ □□□□(□: XQL □□ □□)□ □□□□.

□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□□□.

* B. □□ □□□ □□□ □□□□ □□□□ □□□□ □□, □□□□ □□□□□ □□ □□ □□ □□□ □□□□□ □□□□ □□□□ □□ □□□□. □□ □□□ □□□ □□□ □□□ □□□□□, □□□□□ □□ □□□ □□□□□ □□□□ □□□□. □□□ □□ □□□□□ □□ □□□□ □□□ □□ □□□□□.

* D. □□ □□□ □□□□ □□□□□ □□□ □ □□□ □□ □□, □□□□ □□□□□ □□ □□□ □/□□ □□□□□ □□ □□□ □□□□□. □□ □□□ □□□□ □□□□ □ □□□□ □□ □□□□ □□□□□ □□□ □□□□□. □□□□□ □□ □□□□□ □ □□ □ □□□ □□□□□ □□ □□□□□ □□□□ □□□, □□□□□ □□ □□□ □ □□ □□□□ □□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□□.

□□□ □□□ □□ □□:

Cortex XDR □□ □□□□□ □□□□ □□□ □□ □□□ □□ □□□□□. "□□ □□□ □□□□ □□□□ □□ □□□ □□□ □□ □□ □□□□ □□□ □□□ □□□ □□□ □ □□□□. □□□□□ □□ XQL □□□□ □□ □□□□□ □□□□ □□□ □□□□□ □□ □□□ □□□ □ □□□□□." (□□□□□ □ □□ □□ □□□ □□). EDU-262:

Cortex XDR □□ □ □□ □□□□□ □□□□ □□□ □□□, "□□ □□□ □□□ □□□ □□□□□, □□□□□ XQL □□ □□ □□ □□□□□ □□ □□□ □□□ □□□□ □." (□□ □□□ □□). Palo Alto Networks □□ XDR □□□□ □□□ □□ □□□□□□ □ □□ □□□ □□□□□ □□□ "□□□□□ □ □□"□ □□ □□ □□□ □□□□ □□□ □□.

□□ □□:

Palo Alto Networks Cortex XDR □□ □□: <https://docs-cortex.paloaltonetworks.com/>

EDU-262: Cortex XDR □□ □ □□ □□ □□ Palo Alto Networks □□ XDR □□□□ □

□□□□: <https://www.paloaltonetworks.com/services/education>

/□□#xdr-□□□□

NEW QUESTION: 49

Cortex XDR □□□□ □□□□ □□ □□□□□ □□□ □□ □□□ □ □□ □□ □□□
 □□□□□ □□□□ □□□ □□□□□ □□□. □□ □□□ □□□□□?

- A.** □□ □□ □□ □□□□
B. □□□ □□□ □□ □□
C. □□□□ □□□□□ □□
D. □□ □□□□ □□□□

Answer: B (LEAVE A REPLY)

□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□□□ □□ □□ □□□ □□□□
 □□□. □□□□ □□□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □ □□ □□□
 □□ □ □□□□.

NEW QUESTION: 50

□□ □□□ □□□ □□□□ 321□□ □□□□□□ □□□□ □□ □□□□□ □□□ □
 □□□□□. □□□ □□ □□ □ □□ □ □□□□ 244□□ □□□□□□ □□□□□. □
 □□□□□ □□□ □□□□ □□ □ □□ □□□ □□□ □□□□□? (□ □□□ □□□□
 □□.)

- A.** □□ □□□ □□□ □□□ □ □□□□□ □□ 250□□ □□□□□.
- B.** □ □□□ □□□ □□□□□□ □□□ □□ □□□□ □□□ □□ □□□□.
- C.** □□□ □□□ □□□□□□ □□ □□□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□
□□.
- D.** □□□□□□ IP □□, □□□□ □□ □□ □□□ □□□□ □□□ □□ □□□□□ □□
□□ □□□.

Answer: C,D (LEAVE A REPLY)

[illegible]

* □□ □□ (C, D):

* **C. □□□ □□□ □□□□□□ □□ □□□ □□ □ '□□ □□' □□ '□□ □□' □□□□
□ □□: □□□□□□ '□□ □□' □□ '□□ □□' □□(□, Cortex XDR □□□□ □□□□
□□□□ □□ □□)□ □□, Cortex XDR□ □□ □□□□ □□□□ □□□□ □□ □□ □
□□ □□□□□ □□ □□□□□□ □□□ □□□□□ □□□□ □□ □ □□□□.

* D. □□□□□□ IP □□, □□□ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □□ □□□. □□□□□□ □□ □□□ □□□□□ □□□□ □□□ □□□(IP □□, □□ □ □□ □□ □□)□ Cortex XDR □□□□ □□□ □□□□□ □□□□ □□□. □□□□ □□□□ □□□□□ □□□□ □□□ □□ □□□□□□ □□□ □□□□ □□□□.

* □□ □□□ □ □ □□□?

* A. 250GB of Cortex XDR data is stored in the cloud. Cortex XDR data is stored in the cloud for 250GB of data.

250GB of Cortex XDR data is stored in the cloud for 250GB of data.

* B. Cortex XDR data is stored in the cloud for 250GB of data. Cortex XDR data is stored in the cloud for 250GB of data.

Cortex XDR data is stored in the cloud for 250GB of data.

Cortex XDR data is stored in the cloud for 250GB of data. Cortex XDR data is stored in the cloud for 250GB of data.

260: Cortex XDR data is stored in the cloud for 250GB of data. Cortex XDR data is stored in the cloud for 250GB of data.

Cortex XDR data is stored in the cloud for 250GB of data.

Palo Alto Networks Cortex XDR data is stored in the cloud for 250GB of data.

EDU-260: Cortex XDR data is stored in the cloud for 250GB of data.

https://www.paloaltonetworks.com/services/education

/xdr-250gb

NEW QUESTION: 51

Palo Alto Networks NGFW Cortex XDR data is stored in the cloud for 250GB of data.

A. NGFW data is stored in the cloud for 250GB of data.

B. NGFW data is stored in the cloud for 250GB of data.

C. NGFW data is stored in the cloud for 250GB of data.

D. NGFW data is stored in the cloud for 250GB of data.

Answer: A (LEAVE A REPLY)

Palo Alto Networks NGFW Cortex XDR data is stored in the cloud for 250GB of data.

dataset = panw_ngfw_traffic_raw dataset = panw_ngfw_threat_raw

□□□□ □□□: □□ □□□□ □□□□ □□ □□ XQL □□□ □□□□ □□ □□ □ □
□ □□ □□□ □□ □□□ □□□ □ □□□□.

NEW QUESTION: 52

□□□□ □□□□□ □□ □□□ □ □□ □ □□ □□□ □□□ □□□□□? (□ □□□ □□□□□□.)

- A.** □□ □□□□□ □□
B. □□ □□ □□ □□
C. XQL □□ □□
D. □□ □□□□□ □□ □□

Answer: ([SHOW ANSWER](#))

Cortex XDR □ Cortex XSIAM□□ □□□□ □□□□□ □□□□ □□ □□ □□ □□ □
 □□ □□□□ □ □□□□ □ □□□ □□□ □ □□ □□□ □□□ □□□□□ □□□□
 □□□. □□□ □□ □□□ □□□□□ □□□ □ □□□□ □□□ □□ □□ □□ □□□
 □□□ □ □□□ □□□.

□□□ □□□ □□□□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □□□□□□
□□ □□ □□□□□ □□□ □□□□□ □□□ □ □□□□.

□□ □□□ □□□□ □□□□ □□□ □□□ □□(□: IP □□, □□□ □□ □□ □□ □□)□ □□ □□□ □□ □□□ □□□ □□□□ □□□□ XQL □□ □□□□ □□ □□□□ □ □ □□□□.

NEW QUESTION: 53

□□ □□□ □□□ □□ Cortex XDR □□□□□ □□□□ □□□□. □□□□□□ □□□
 □□ □□(□: OS, □□□□, □□□□□) □□□ □□□□□□□□. □□□ □□ Linux □□
 □□ OS □□ □ □□□□ OS □□□□ □□ □□ □□□ □□□□□□□□□?

- A.** ☐☐☐ ☐☐☐ ☐☐☐☐
- B.** ☐☐ ☐☐ ☐☐ ☐☐
- C.** ☐☐ ☐☐ ☐☐ ☐☐
- D.** ☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐

Answer: (SHOW ANSWER)

☐ Linux ☐☐☐☐ ☐☐, ☐☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐ ☐☐

Windows□ macOS□ □□ Linux□ □□□□□ □□ □□□ □□□ □□□□, Cortex XDR
 □□□□□ □ □□□□□□□ □□□□ □□ □□ □□□ □□□□□ □□ □□ □□□ □
 □□□□.

XDR-Engine □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ XDR-Engine □□! DumpTop □ □□ **XDR-Engine** □□ □□□ □□□□□□, DumpTop XDR-Engine □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop XDR-Engine □□□ □□□□□.

<https://www.dumptop.com/Palo-Alto-Networks/XDR-Engineer-dump.html> (83 Q&As
Dumps, **30%OFF** Special Discount: **KrDump**)