

PaloAltoNetworks.XSIAM-Engineer.v2025-11-12.q101

□□□□:	XSIAM-Engineer
□□□□:	Palo Alto Networks XSIAM Engineer
□□□:	Palo Alto Networks
□□ □□ □□□:	101
□□:	v2025-11-12
# □□ □:	106
# □□ □□□:	1010
https://www.krdump.com/PaloAltoNetworks.XSIAM-Engineer.v2025-11-12.q101.html	

NEW QUESTION: 1

□□□ XSIAM □□□ □□□ □□ □□(□: □□ IP, □□ □□□ □□□)□ □□□□ '□□' □□ □□ □□□□□ □□□□ □□□□□ □□□□□□□□. □□□ □□ □, □□□ □□□ □□□□ □□□ □□□ □□ □□□□□ □□□□□ □□ □□□□□ □□□□ □□ □□ □□□ □ □□ □□. XSIAM □□□ □□□□ □□□ □□□□ □□□□□. □□ □□□□□ □□□□ □□□ □□ □□□□ □□ □□□□ □□□ □□□ □□□□□?

- A. □□□ □□□ □□□□ '□□' □□ '□□'□ □□□ □□□ □□□ □□□□□ □□□ □□, □□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□□□.
- B. □□□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□(□□ □□□ □□ □□)□ □□□ □ □□□ □□□ □□□□ □□□ □□□□□ □□□□□.
- C. □□□ □□ XSIAM '□□□□ □□'□ □□□□ □□□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□ □□□ □□□ □□□□.
- D. □□□ □□□ □ □□ □□□ □□□□ □□□□ □ □□□ □□□□□ □□□□□ □□□ □□ □□□□□.
- E. □ □□ □□□ □□□ □□□ □□ □□ □□ □□□□ □□ □□□ □□□ □ □□ □□ □□ □□□ □□ XSIAM □□□ □□□ □□□ □□□□□.

Answer: ([SHOW ANSWER](#))

□ □□□□□ □□□ □□□ □□□□ □□□□□. □□□ □□ □□□□ □□□ □□□□ □□ □ □□□ □□□ □□ □□ □□□ □□ □□□ □□□□. □□ □□□□ □□□(B)□ □□□□ □ □□□ □□ □□□□ □□□ □□, □□□□ □□ □□ □□ □□□□ □□□ □ □□ □□□ □□ □□□□ □□ □□□ □□□□□ □□□ □ □□□□ □□ □□□□□□. □□ ED □□□□ □. XSIAM □□□ □□□ □□ □□(□□□□□ □□)□ □□□□□. □□ □□□ □□□□ □□ □ □□□ □□□□□ □□□□ □□(□: □□ □□ □□ □ □□) □□ □□□ □□□□□ □□ □ □□□□. □□ A□ D□ □□ □□□ □□□□□ □ □□□□□ □□□ □□□ □□□ □□ □□ □□ □□□□ □□□□□. □□ C□ □□□ □□□ □□□ □□□□□, □□□□□ □□□ □ □□ □□ □□□□□ □□□□□ □□ □□ □□□□□.

NEW QUESTION: 2

A SOC analyst at Palo Alto Networks XSIAM is reviewing logs from AbuseIPDB, VirusTotal, and other threat intelligence sources. The analyst notices several IP addresses that appear to be associated with malicious activity. Which of the following actions should the analyst take to investigate these IP addresses further?

- A. Use XSOAR to automatically generate and execute a series of commands to probe the IP addresses.
- B. Use XSOAR to automatically generate and execute a series of commands to probe the IP addresses, but only if the IP addresses are associated with a known threat.
- C. Use a tool like YARA to generate a rule that can detect malicious activity associated with the IP addresses, and then use the rule to scan the logs.
- D. XSIAM is a cloud-based SIEM, so the analyst should use the XSIAM console to investigate the IP addresses.
- E. Use XSOAR to automatically generate and execute a series of commands to probe the IP addresses, but only if the IP addresses are associated with a known threat and the analyst has the necessary permissions.

Answer: E (LEAVE A REPLY)

Explanation: XSIAM is a cloud-based SIEM. While it can integrate with XSOAR, the analyst should use XSOAR to automatically generate and execute a series of commands to probe the IP addresses, but only if the IP addresses are associated with a known threat and the analyst has the necessary permissions. This is the most secure and controlled way to investigate the IP addresses. Option A is incorrect because it suggests automatically executing commands without any checks. Option B is incorrect because it suggests only executing commands if the IP addresses are associated with a known threat, but the analyst should also consider the context of the logs. Option C is incorrect because YARA is a tool for generating rules to detect malicious activity, but it is not the best way to investigate specific IP addresses. Option D is incorrect because XSIAM is a cloud-based SIEM, but the analyst should use XSOAR to investigate the IP addresses.

NEW QUESTION: 3

A Linux system administrator is configuring XSIAM to monitor for HTTP requests from a specific IP address. The administrator wants to use a regular expression to match the IP address. Which of the following regular expressions is the correct one to use?

- A.
- B.
- C.

{< >}:

- D.

Answer: D (LEAVE A REPLY)

Explanation: The correct regular expression to use is {< >}. This regular expression matches any two characters between angle brackets. The administrator wants to monitor for HTTP requests from a specific IP address, so the regular expression should match the IP address. Option A is incorrect because it does not match the IP address. Option B is incorrect because it does not match the IP address. Option C is incorrect because it does not match the IP address.

□ □□□□ □□ 'group-name'□ □□ □□□□□ □□□□□. □□ □□□ □□□□□□ □□ □ □□ □□□ □□□ □□ □□□□□. □ □□□ XSIAM □□□□ □□□□ □□□□ □□□ □□ □□□. HTTP PROXY □□ □□□ swgetTcurl&□ □□□ □ □□□, □□□□ □□ □□□□ □ □□ □□□ □□ □□□□ □□□□□ □□□□□. 'token' □□□□□ □□□□□ □□ XSIAM □□□□□ □□□□□ □ □□□□□□□. □□□□ □□□□□ □□□ XSIAM □□□□ □□ □□ □□ □ □□□, '--proxy-string', '--group-name' □ '--token'□ □□ □□□□□.

NEW QUESTION: 4

XSIAM □□□□□ □□□□ □□□ □□□□□ □□□□□□□□. □□□ □□□ □□□ □□ □□ □□□□ □□□□ □□□□. □□□□ □□□□ □□□ '□□□□□ □□'□□□□. Cortex XDR □□ □□□□ □□□□ Windows □□□□□□□ □□□□□□ □□□□□ □□ □ □□ □□□ □□□□ □ □□?

- A. □□□□□□□ XSIAM □□□□□□□□□ □□ □□ RDP □□□ □□□ □□□.
- B. □□□□□□□ Cortex XDR □□□□□□ '□□□□□ □□' □□□ □□□ □□□.
- C. XSIAM □□□□□ □□□□□□ □□ □□□□□□ □□ □□ □□□□ □□□ □□□ □□□.
- D. Cortex XDR □□□□□□ □□ □□□□□ □□, XDR □□□□□□ □□□□□ □□□ □□□, '□□ □ □□' □□□ □□□□□□ □□□ □□□.
- E. □□□□□□□ □□□□ XSIAM □□□□□□□□□□ ICMP □□□□□ □□□□□□ □□□□□ □□ □.

Answer: D (LEAVE A REPLY)

'□□□□ □□' □□□ □□□□□□ Cortex XDR □□□□□□ □□ □□□□□ □□, XDR □□□□□ □□ □□ □□□□ □□□ □□□ □□ □□□ □□□ □□□. '□□□□□ □□' □□□ □□□ □□□□□□. RDP □□□, XSIAM □□□□□□□□□□ □□ □□□□□ □□(XDR □□□□□□□ □□□□□□□□□ □□ □ □□□ □□ □□□ □□□□□ □□□□ □□□), □□□□ ICMP □□□□ □□□ □□□ □□ □□ □□ □□ □□ □□□□.

NEW QUESTION: 5

□ □□□ XSIAM □□□□□□□ □□□ □□□ □□ □□□□□ □□□ □□ S3 □□□ □□ '□□ □□□ □□ □□□ □□□□ □□' □□□ □□□□ □□□□ □□□□. □□□ □□□□ □□□ □□□□ □□□ □□□□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□ □□ □□□□ □□□ □□ □□□□□ □□□ □□□□ □□□ □□ □□□□□ □□□ □□□□□□□□□□?

- A. □□□ □□□□□□ '□□□□□□ □□ □□□ □□□□ □□' ASM □□□□ □□□ □□□□□□ □□.
- B. □□ ASM □□ □□ □□ □□ S3 □□ □□□□□ □□□ □□ □□ □□□ □□□□.
- C. '□□□□□□ □□ □□□ □□□□ □□' □□□□ XQL □□□ □□□□ □□ □□□□□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□.
- D. □ □□ S3 □□□□ □□ □□ □□□□ '□□□' □□ '□□□'□ □□□□□□.
- E. □□ □□ □ □□□ □□ S3 □□□□ □□ □□□ □□□□ □□□□□ □□□□ SOAR □□□□□ □□□ □□□.

Answer: (SHOW ANSWER)

B C ASM ... B(XQL ...) 'public_content_delivery' ... A ... D ... E ...

NEW QUESTION: 6

XSIAM ... ' ... XQL ...

... ? (...)

A. Visual Studio ...

B. ... 'risk_score' ...

C. ... 'target_process_integrity_level = 'System' ... 'injection_type = 'remote' ... XQL ...

D. ...

E. ... ' ... ' ...

Answer: A,C,D (LEAVE A REPLY)

A, C, D ... (false positive) ... A: parent_process_name ... C: ... 'injection_type' ... (XDR ... ' ... ') ... D: ... / ... : ... B(risk_score ...) ...

□□ □ □□□□□□□. IP □□□(□□ □□)□ □□□ □□ □□□ □□□□□ □□□ □ □□□ □.

NEW QUESTION: 10

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

- A. □□□ □□
- B. □□□
- C. □□
- D. □□

Answer: B,C (LEAVE A REPLY)

Cortex XSIAM□ □□□□ □□□□ □□□ □□□□ Slack□ □□ □□ □□□□ □□□ □ □□ □□. □□□ PagerDuty□ SMS □□□□ □□□□□ □□ □□□□□□□□ □□□□□.

NEW QUESTION: 11

□□□ □□□□ XSIAM□ □□□□ □□□ □□□□ □□ □□□□□ □□□□□□□. XSIAM□ □□ □□ □□ □ □□□ □□ □□ □□□ □□□□□, □□□□ □□ □□(□: □□□ □□□ □ □□□□ □□□ □□□ □□ □□ □□ □□)□ □□ □□□ □□□□□ □□□□□ □□ □□ □□ □□□ □□□ □□□ □□□□□ □□□□□ □□□□ □□□ □□□ □□□ □□□ □□□□□ □□□□ □□□ □□□ □□□□□. □ □□ '□□(JIT)' □□ □□ □□ □□□ □□□□ □□ □□□□ □□□□ □ □□ □□□ XSIAM □□ □□ □□ □□□ □□□□□?

- A. XSIAM□ PAM □□□□□ □□ □□ □□□□ □□ □□□ □□□ □ □□ PAM(Privileged Access Management) □□□□ XSIAM□ □□ □□□ □□□□□.
- B. □□ □□ □□ □□□□ '□□□□' □□□ □□□□ □□□□□, □□ □□ □□□ □□□□ □ □□□□. □□□ □□ □□ □□□ □□□□□.
- C. □□ □□□ □□□ □□ 'Break Glass' XSIAM □□□ □□□ □□□□□. □ □□□ □□ □□□ □□□□ □□ □ □□□□ □□ □□□□□ □□□□□.
- D. □□ □ XSIAM API□ □□ □□ □□ □□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□ XSIAM □□□ □□□□□ □□□□□.
- E. □□ □□□ □□□□□ □□ □□□ □□ □□ XSIAM □□□□□ □□□ □□□ □□□□ □ □ IdP □□□□ □□□□□.

Answer: A,D (LEAVE A REPLY)

A□ D □□ □□ □□ □□□ □□□□□. □□ A□ □□□□ □□□□□□□□ □□□□□□. XSIAM□ PAM □□□(□: CyberArk, HashiCorp Vault □)□ □□□□ □□□□ □□□□ □□ □□□□ □□□□. PAM □□□□ □□ □ □□ □□□□□ □□ □□ □□ □□ □□□ □□□□ □□□ □, XSIAM□ □□□ □□ □□ □□□□ □□□ □□□ □ □□□□. □□ □□ □□□□ □□□ □□□□□. □□ D□ XSIAM □□□ □□ □□□□□ □□□□□□□□ □□ □□□□□. XSIAM □ □□□ □□□□ API□ □□□□ □□□ □□□ □□□□ □□□□□ □□□ □ □□□□. □□ □□□□ □□□ □□□ □□□ □□□□□ □□ □□□□□. □□ B□ □□ □□□□ □□ □□ □ □□□□ □□, □□□□ □□□□ □□□□□. □□ C□ □□□□□ □□□ □□□□□.

Which of the following is a benefit of using XSIAM for authentication? (Select two.)
A. XSIAM can be used to authenticate users to network devices.
B. XSIAM can be used to authenticate users to applications.
C. XSIAM can be used to authenticate users to cloud services.
D. XSIAM can be used to authenticate users to physical devices.

NEW QUESTION: 12

Which of the following is a benefit of using XSIAM for authentication? (Select two.)
A. XSIAM can be used to authenticate users to network devices.
B. XSIAM can be used to authenticate users to applications.
C. XSIAM can be used to authenticate users to cloud services.
D. XSIAM can be used to authenticate users to physical devices.

- A. XSIAM can be used to authenticate users to network devices.
- B. XSIAM can be used to authenticate users to applications.
- C. XSIAM can be used to authenticate users to cloud services.
- D. XSIAM can be used to authenticate users to physical devices.
- E. XSIAM can be used to authenticate users to mobile devices.

Answer: B (LEAVE A REPLY)

Which of the following is a benefit of using XSIAM for authentication? (Select two.)
A. XSIAM can be used to authenticate users to network devices.
B. XSIAM can be used to authenticate users to applications.
C. XSIAM can be used to authenticate users to cloud services.
D. XSIAM can be used to authenticate users to physical devices.

NEW QUESTION: 13

Which of the following is a benefit of using XSIAM for authentication? (Select two.)
A. XSIAM can be used to authenticate users to network devices.
B. XSIAM can be used to authenticate users to applications.
C. XSIAM can be used to authenticate users to cloud services.
D. XSIAM can be used to authenticate users to physical devices.

- A. 'XXXX XX' XXXX XXXX XXXX XX IP XXXX XXXX XX XXX XX XX XXX XXXX.
- B. XXXX XXXX XX' XXXX(XX XXXX XX XX) 'XX' XXXX(XXXXXXXX XXXX XX) 'XXXX XXXX' XXXX(XXXX XX XX) XXXX XXXX XX XX XXXX XX XX, XX XX XX XXXX XX XX XXXX XXXX.
- C. XSIAM XXXX XX XXXX XXXXXXXX XXXX XX XXXX XXXX XX XXXX XXXX XXXX.
- D. XX XXXX XXXX XXXX XXXX XXXX XX XXXX XX XXXX(UEBA) XXXX. UEBA XXXX XXXX XXXX XXXX XXXX.
- E. XXXX XXXX XX XXXX XXXX XX XXXXXXX XXXX XXXXXXXXXX XXXX XXXX XX XXXX XXXX XX XXX XXXX.

Answer: (SHOW ANSWER)

B XXXX XXXX. XXXX, XX, XXXX XXXX XX XXXX XXXX XXXX XXXX XXXX XXXXXXXX XXXX XXXX XXXX XXXXXXX XXXXXXX. XXXX XXXX XXXX XXXX XXXXXXX XXXX XXXX XXXX XXXX XXXX. A E XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX. C XXXX XXXX XXXX XXXX. D IJEBAX XXXXXXX, XXXXXXX XX XX XX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX.

NEW QUESTION: 14

XXXX XXXX XXXX XSIAM XXXX XXXX XXXX XX XXXX XXXX XX XXXX Amazon Kinesis Data Stream XXXX XX XXXXXXX. XSIAM XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXXXXX?

- A. Lambda XXXX Kinesis XXXX XXXXXXX XXXX, XXXX XXXX XSIAM XXXX AWS S3 XXXX.
- B. AWS Kinesis Firehose XXXX XXXX Palo Alto Networks XSIAM HTTP XXXXXXX XXXX XXXX.
- C. Kinesis XXXXXXX XXXX syslog XSIAM XXXX XXXX XXXX XXXX XXXXXXX XXXX EC2 XXXXXXX.
- D. Kinesis XXXX CSV XXXX XXXX UI XSIAM XXXX .
- E. Kinesis Lambda XXXX XSIAM XXXX AWS CloudWatch Logs XXXX XXXX.

Answer: B (LEAVE A REPLY)

B HTTP XXXX XXXX XXXXXXX AWS Kinesis Firehose XXXX XXXX, Kinesis XSIAM XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXX . Firehose HTTP XXXXXXX XXXX XXXX XXXXXXX XXXXXXX XXXX XXXX XXXXXXX. A S3 XXXX XXXXXXX XXXXXXX XXXXXXX XXXX XXXX . C XXXX XXXX XXXX XXXXXXX. D XXXX XXXXXXX .

□□□ □□□□. □□ E□ □□ □□□□□, Firehose□ □□□□□ □□□□□□ □□ □□□□ □ □ □□□ □□□ □□□□.

NEW QUESTION: 15

'□□□□□□ □□' □□□ □□ □□□ □□ XSIAM □□ □□□ □□□ □□□.

'app_crash_detection'□ □□ □□ □□□ □□ □□□ □□□□□. 'alert.count = 1',

'alert.app_name = 'ERP'', 'alert.environment = 'prod'', □□□ □□ □□□ □□ □□ □□ '50'. □

□□□ □□ □□□ □□□□□?

- A. 65
- B. 90
- C. 95
- D. 100
- E. 75

Answer: C (LEAVE A REPLY)

□ □□□ XSIAM □□ □□ □□□ □□ □□□ □□□□ □□□□, □□ '□□ □□□' □□□□ □□□□□. □□ □□(50□ -> 80□, 120□)□ □□ □□□ □□ □□□□□ □□□□ □□ □□ □□□ □□ □□□, □□ □□ □□ □□□(□□ □□ □□ □□□ □□□ XSIAM □□)□□□ □□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□ □□□□ □□ □□□ □□□ □□ □□□□. □□□ '□□□' □□□ □□ 95□□ □□ □□□□ □□ □□ □□□ □□□ □□□ □□. 1. □□ □□ □□: 50□ 2. □□ □□ 3: '□□ □□ □□'(□□: 5) □□: alert.detection_rule_id = 'app_crash_detection' AND alert.environment = 'dev' □□ □□ 'alert.environment'□ 'prod'□□□. □□: □□□ □□□□□. □□ 3□ □□□□ □□□□. □□ □ □□ 50□□□□. 3. □□ □□ 1: '□□ □□'(□□: 10) □□: = 'app_crash_detection' AND alert.count > 1 0' □□ □□ 'alert.count'□ 15(10□□ □ □)□□□. □□: □□□ □□□□. □□: □□ □□ □□: +30. □ □□□□ □ □□□ □□ □□ □□□□ +30□□□. □□ □□ □□(□□ □□ □) □□ □□□ □□□ □□ □□): 50 + 30 = 80.4. □□ □□ 2: '□□ □□□□□□ □□' (□□: 20) □□: 'alert.detection_rule_id = 'app_crash_detection' AND alert.app_name in ('ERP', 'CRM')' □□ □□ 'alert.app_name'□ 'ERP'(□□□ □□)□□□. □□: □□□ □□□□. □□: □ □□ □□: xl .5. □□□ □□□ □□ □□ □□: □ □□□□ □□, '□□ □□ □□'□ □□□ □ □□ □□□ □□□ □□ □□□, □ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□ □ □□ □□□ □□□□ □□□ □ □□□□. 'xl .5'□ '□□ □□'(□□ 1)□□ +30 □□□□ □□□□ □□, □ □□ □□ 'app_crash_detection'□ '□□ □□□□□□ □□'□ □□□ □□ □□□□□. 'Crash'□ □□ □□ '□□' □□□ □□□□□. □□ 1□ □□ □□□□ 1.5 = 45'□ □□□. □□□ □□□ '□□ □□ □□ + □□ □□□ = 50 + 45 = 95'□ □□□. □□□ □□□ □□□ 95□ □□ □□, '□□ □□'□ □□ □□□ □□□ □□□□ □□□ □ □□ □□□ □□□ □□ □□□□□ □□ □ □ □□ □□ □□□ □□ □□□ □□□□□. □□□ □□ □□ □□ □□ □□□□ 120□ (□□ 100□)□ □□□, 95□□ □□ □□ □□ □□□ □□ □□□ □□□□□.

NEW QUESTION: 16

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

- A. `asset.tags CONTAINS 'FinTech' AND 'process.hash IN EDL('FinTech_Benign_Hashes')`
- B. `'source_bu = 'FinTech' AND 'process.hash IN ('hash1', 'hash2', ...y')`
- C. `asset.tags CONTAINS 'FinTech' AND 'process.hash IN EDL('FinTech_Benign_Hashes')`
- D. `'alert_name = AND 'source_ip IN 'XSIAM 'asset.tags CONTAINS 'FinTech'`
- E. `asset.tags CONTAINS 'FinTech' AND 'process.hash IN EDL('FinTech_Benign_Hashes')`

Answer: (SHOW ANSWER)

Correct answer: A, C, D, E. XSIAM queries are valid if they use the correct syntax for the operators and functions. Option A is a valid query. Option B is invalid because the single quote is not properly escaped. Option C is a valid query. Option D is invalid because the AND operator is not properly used. Option E is a valid query.

NEW QUESTION: 18

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

- A. XSIAM queries are valid if they use the correct syntax for the operators and functions. XSIAM queries are valid if they use the correct syntax for the operators and functions.
- B. XSIAM queries are valid if they use the correct syntax for the operators and functions. XSIAM queries are valid if they use the correct syntax for the operators and functions.
- C. XSIAM queries are valid if they use the correct syntax for the operators and functions. XSIAM queries are valid if they use the correct syntax for the operators and functions.

- D. XML `<url>` tag is not present in XSIAM log.
- E. XML `<severity>` tag is not present in CVSS score in XSIAM log.

Answer: (SHOW ANSWER)

Option A is incorrect because XSIAM logs are in XML format. Option B is incorrect because XSIAM logs are in XML format (XML to XSLT conversion). Option C is incorrect because XSIAM logs are in XML format (CVSS score, source IP). Option D is incorrect because XSIAM logs are in XML format. Option E is incorrect because XSIAM logs are in XML format.

NEW QUESTION: 19

Cortex XSIAM Cloud Identity Engine `pan_dss_raw` field?

- A. Cortex XSIAM `pan_dss_raw` field is not present in logs.
- B. Cortex XSIAM `pan_dss_raw` field is present in logs.
- C. Cortex XSIAM `pan_dss_raw` field is present in logs.
- D. Cortex XSIAM `pan_dss_raw` field is not present in logs.

Answer: C (LEAVE A REPLY)

The `pan_dss_raw` field is present in Cortex XSIAM logs from Cloud Identity Engine.

NEW QUESTION: 20

Which of the following is not a valid XSIAM action? (Select all that apply)

- A. XSIAM `pan_dss_raw` field is not present in logs.
- B. XSIAM `pan_dss_raw` field is not present in logs.
- C. NGFW `TIP API` is not a valid XSIAM 'Action'.
- D. API `pan_dss_raw` field is not present in logs.

E. XSIAM '□□□ □□□'□ □□ □□ □ □□□ IOC □□□□ □□□ □□ □□ □□ □ □ □□ □□ □□□□ □□□□□.

Answer: A,B,C,D,E (LEAVE A REPLY)

□ □□□□□□ □□ XSIAM □□□ □□□□ □□□□ □□ □□□ □□□□□. A: XSIAM□ □ □ □□□□ □□□ □□□□□, □□□ □□□ □□□ □□ □□□ □□□□□. B: □□□ □ □□ □□□ □□□ □□□ □□ □□, □□□, □□ □ □□ □ □□□ □□ □□□□ □□ □□ □□□ □□□□□. C: XSIAM '□□' □□□ □□□ □□ NGFW □ □□□ □□□ □□ □ □ TIPO □□ □□□□ □ □□□□□□. D: API □□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□□□ □□□□ □□□ □□ □□□ □□□□□□. E: □□□ □□□ □□□ □□ □□ □□, □□ □ □□□ □□ IOC □□□□ □□ □□ □□ □ □□ □□□ □□ □□□□□.

NEW QUESTION: 21

XSIAM □□□ □□□ □□ □ JSON □□□□ □□□ □□□□ □□ □□ □□□□□□□ □□□ □□ □□□ □□□ □□□□□. □□□ □□□□□□□□ □□ □□□ □□ □□□ □□□ □□ □□ XSIAM□□ □□□□ □□□□□ □□□ □□□ □□□□□. □□□ □□ XSIAM □□ □□ □□□ □□ □ □□□□ □□□□□ □□□□ □□□□. □□□ □□□ □□ □□□ □□□□□. □□ □ □□ □□□ □□ □□□ □□ □□□ □□□□, XSIAM □□□□□ □□□ □□□ □□□ □ □□□?

- A. XSIAM □□□□ □□□ □□ □□□ □□ □□ □□□ □□□ JSON □□□□ □□□ □ □□ □□. □□ □□□ □□ □□□□ □□ □□ □□□ □□□□.
- B. XSIAM□ □□ □ □□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□□. 'message' □ □□ □□□□□□ □□□ □□('ln')□ □□□ □□□ □□□□□ □□□□ □□□ □□□□□. XSIAM □□ □□□□ □ JSON □□□ □□('A(S) □□ □□□ CAY□ □)□ □□□□□ □□□□ □□ □□□ 'multiline_regex'□ □□□□□.
- C. JSON □□□□ XSIAM□□ □□ □□□ □ □□ □□□ □□□□ □□□ □□□□ □□□□. □□□□ □□□□ □□ □□ □□□ UTF-8□ □□□□□.
- D. □□ □□□□□□□ XSIAM □□□□ □□□ □ □□ □□□□ □□□ □□□□ □□□□ □ □□□ □□□□□ □□□□. □□□□ □□ □□□ □□□□□ □□ □□□ □□□□□.
- E. XSIAM□ □□□ □□ □□□ □□ □□□ 'details.message' □□□ □□ □ □□□□ □□ □ □□□□ □□□□ □□ □□□ □□□□□. □□ □ □□□□□ CLOB □□□ □□(□□□□ □□) □ □□□ □ □□□ □□□□ □□□□□.

Answer: B (LEAVE A REPLY)

□ □□□□□ □□ □ □□□□ □□ □□□□ □□, □ □□ □□□□ □□□□□. □□ □ □□ □ □□ □□□ □□□ □□□□ □□, □□ □□ □□□□□□□ □□□ □□(C'n')□ □□□□ □□ □ □□□ □ □□□□. □□ B□ □ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ 'multiline_regex'(□: □ JSON □□□ □□ □□ □□)□ □□□□□. □□ A□ □□□ □ □□ □□□□□. □□ C□ □□□ □□ □□□ □□□□□□□. □□ D□ □□ □□□□ □□□/ □□□ □□ □□□ □□□ □□□□□. □□ E□ □□ □□ □ □□□ □□ □□□ □□ □□ □ □□□ □□□ □□ □□□□.

- C. NGFW XSIAM Collector □□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□□.
- D. XSIAM □□□ □□□□□ □□ □□ □□ □□□ □□□□ □□ □□□□ □□□□ □□ □□ □□ '□ □ □□' □□ □□□□□.
- E. □□□ □□ □□ □□□ □□ XSIAM □□□ □□□□□□ 'sapp_id'□ □□ □□□□ □□□ □. □ □□□ □□□ □□□ □□ □□□ □□□□ □□□ □□□□□□.

Answer: (SHOW ANSWER)

Palo Alto Networks NGFW□ □□ PAN-OS □□□□□□ □□ □□ □□□ □□□ □ □□□□. XSIAM□ Palo Alto Networks □□ □□ □ □□□□ □□ □□ □□□ □□□ □□ □□□□□. □ □□□□□ 'app_id'□ □□□□□ □□□□□ □ XSIAM□□□□ 'unknown'□□ □□□□ □□, □□ □□□ □□ □□ □□(□□ □□ □ □□ □□ □□ □□)□ □□□□□□ □□□ □□□□ □.

□□ A□ B□ □□ □□□□□ □□□ □□□□□. □□ C□ □□ □□□ '□ □ □□' □□ □□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□. □□ D□ □□ □□□ □□□ □□□□, □□ □□□ □□□□□ □□□ □□□ □□□□. □□ E□ □□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□□, □□ NGFW □□□□□□ □□□ □ □□□□□ □ □□□□□ □□□□ □□□ □□□□□.

NEW QUESTION: 26

- CISO□ □□□ □□ 3□ □□ □□, MITRE ATT&CK □□, □□□ □□ □□ □, □□□ □□□ □ □□ □□ □□ '□□'□ □□□□ □□□ XSIAM □□ □□□□ □□□□□. □ □□□□ □□ □ □□ □□ □□□□ □□ PDF □□□ □□□□□ □□□. □□ □□□□□□ □□ XSIAM □□□ □□□□ □□□?
- A. □□ □□ □□ □□□□ □□□ □□□ □□□□□ □□□□ PDF□ □□□□□□.
 - B. XQL □□□ □□□□ □□□ □□ □□□ □□□□ □□□□(MITRE ATT&CK □□□□□ □ □ topk□ join□ □□□□, □□□□□ □□□ □□), □□□ □□□ □□ '□□' □□□□ □□□ □, PDF □□□□ □□□□ □□□□ □□□□□ □□□□□.
 - C. □□□ '□□ □□' □□□□ □□□□ □□ □□ □□□ □□□ □□□ □□□□.
 - D. API□ □□ □□ □□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□□.
 - E. □□□□ □□ □□ □□□ □□□ CISO□ □□ □□□ □□□ □□□□□.

Answer: (SHOW ANSWER)

□□ □□□ □ □□ □□ □□□ □□□□ □□□□ □□ □□□□ □□□□□□ XSIAM□ □□ □□ □□□ □□□□□. □□ B□ □□□ □□□ □□□□ □□□□□. □□□ □□ □□□ □□ □□□□ □□□ XQL □□□ □□□□ □□ □□, □□ □□□ MITRE ATT&CK □□(MITRE □□□ □□ □□ □□□ □□□□ □□□ □□), □□□ □□□ □□ □□ □□□ □□□ □ □□ □□. □□□ □□□ □□□ □□ '□' □□□□ □□□ □□□. □□ XSIAM□ □□□ □□□□ □ □□ PDF □□□ □□ □□□ □□□ □□□□□ CISO□ □□□ □□ □□□□□. □□ A, C, D, E □ □□□□□, □□□□□□, XSIAM□ □□ □□ □□ □□□ □□□□.

NEW QUESTION: 27

Which of the following is the most effective way to protect sensitive data stored in a cloud storage service? XSIAM is a cloud storage service. Which of the following is the most effective way to protect sensitive data stored in a cloud storage service? XSIAM is a cloud storage service. Which of the following is the most effective way to protect sensitive data stored in a cloud storage service?

- A. 'Data encryption' is 'encryption key' management software to manage encryption keys PDF encryption software.
- B. Cloud storage services provide 'data backup' services to backup data and restore data.
- C. Cloud storage services provide IPsec to protect data transmission between cloud storage services and users. Cloud storage services provide XQL to protect data transmission between cloud storage services and users. PDF and CSV files are encrypted and stored in the cloud.
- D. 'Data backup' services provide backup services to backup data and restore data.
- E. API is used to manage data in the cloud storage service. XSIAM provides a secure way to manage data in the cloud storage service.

Answer: C (LEAVE A REPLY)

Cloud storage services provide IPsec to protect data transmission between cloud storage services and users. Cloud storage services provide XQL to protect data transmission between cloud storage services and users. network_connection_logs is a log file that contains IP addresses and other information. Cloud storage services provide PDF and CSV files are encrypted and stored in the cloud. API is used to manage data in the cloud storage service. XSIAM provides a secure way to manage data in the cloud storage service. Cloud storage services provide backup services to backup data and restore data.

NEW QUESTION: 28

XSIAM is a cloud storage service. Which of the following is the most effective way to protect sensitive data stored in a cloud storage service? XSIAM is a cloud storage service. Which of the following is the most effective way to protect sensitive data stored in a cloud storage service? XSIAM is a cloud storage service. Which of the following is the most effective way to protect sensitive data stored in a cloud storage service? XSIAM is a cloud storage service. Which of the following is the most effective way to protect sensitive data stored in a cloud storage service?

- A. ICS is a protocol used for data transmission between ICS and XSIAM. ICS is a protocol used for data transmission between ICS and XSIAM. ICS is a protocol used for data transmission between ICS and XSIAM.
- B. ICS is a protocol used for data transmission between ICS and XSIAM. ICS is a protocol used for data transmission between ICS and XSIAM. ICS is a protocol used for data transmission between ICS and XSIAM.
- C. ICS is a protocol used for data transmission between ICS and XSIAM. ICS is a protocol used for data transmission between ICS and XSIAM. ICS is a protocol used for data transmission between ICS and XSIAM.
- D. XSIAM is a cloud storage service. XSIAM is a cloud storage service. XSIAM is a cloud storage service. XSIAM is a cloud storage service. XSIAM is a cloud storage service.
- E. NAT is a protocol used for data transmission between NAT and XSIAM. NAT is a protocol used for data transmission between NAT and XSIAM. NAT is a protocol used for data transmission between NAT and XSIAM.

Answer: A (LEAVE A REPLY)

ICS 系统，通过（...）... ICS 系统... (C, E), ... (B), ... (D).

NEW QUESTION: 29

XSIAM ... IP 60 ... 5 ... SOC ... 'OR' ... 'root' ... XSIAM ... 'target_user' ... 60 ... 30 ... 5 ...

- A. ...
- B. ... 'OR' ... 'root' ...
- C. ... 'target_user' ...
- D. ... 60 ... 30 ...
- E. ... 5 ...

Answer: C (LEAVE A REPLY)

C ... JSON ... Broker VM ... Cortex XSIAM ... JSON ... XSIAM ... Broker VM ... UDP 514 ... JSON ... syslog ... XSIAM ... JSON ...

NEW QUESTION: 30

JSON ... Broker VM ... Cortex XSIAM ... JSON ... XSIAM ... Broker VM ... UDP 514 ... JSON ... syslog ... XSIAM ... JSON ...

- A. UDP 514 ... JSON ... Broker VM ... syslog ... XSIAM ... JSON ...

00 C0 00 0000 00000 000000. 00 0000 00000 00000 00000 00 00
00 0000 0000 000000. 00 0000 000000 00 0000 00000 0 0000 0000
0000. 00 0000 IP 0000 00 00 0 0000 0000 000000 00 00 0000 00 0
0000 00000 0000 00 00000 00 00 0000000. 00 00 0000 00 00000
0000 00 00000 0000 0000 00 0000 0000000 00 0000 00 00000 0000
00 00 0 00000. 00 A: 00000 0000 00 0000 00 00 TI 00000 00 0000
0 00000. 00 00 00 0 00 0000 00/00 00000 00000 000000. 00 B: 0
0000 0000 00 00 0000 000000. 0 0000 0000 00 00 00000 000000 0
0 0000 00 0000 0000 0000 00000 00000. 00 D: XSIAM0 0000000 0000,
00 0000 00000 00 0000 00 00 0000 0000 0000 00000 00000 00 00
0 00000 00000. 00 E: 00 0000 0000 000000000 0000000 00 0000 00
00 00000. 00000 0000 00000 00000 0000000 0000 00 0000 000000.

XSIAM-Engineer 00 0000 0000000 00 DumpTop 00 00000 0000 XSIAM-Engineer 00! DumpTop 0 00 **XSIAM-Engineer** 00 0000 00000000, DumpTop XSIAM-Engineer 00 0000 00000000000 0000 0000000000. 000000 0000 00 00 00 DumpTop XSIAM-Engineer 0000 0000000. <https://www.dumptop.com/Palo-Alto-Networks/XSIAM-Engineer-dump.html> (436 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 32

0000 APT 0000 DNS 00000 0000 0000 00 0000 00000 0000 0000 00000. 0000 0000000 000000 0000 0000 DNS 00 00 00000 0000000 00 00 0 0 (C2) 0000000 0000000, 0000 000000 000000 0000000000000 0 0 00000 00000. XSIAM00 00 0000000 00 0000000 BIOC 0000 00000 00 0. 0 0000 00 DNS 00 0000 00 0000 000000 0 0 0000 0000000 0000000 0 00 000000 DNS 0000 0000 0000 0000. 0 BIOC0 00 00(false positive)0 00 00000 00 00000 XSIAM XDR 0000 00 0000 0000 0000000?

- A.
 - B.
 - C.
- {<0>}:
D.

Answer: C (LEAVE A REPLY)

00 C0 DNS 000000 000000 0 00 0000000 0000 BIOC0000. 00 A0 0000 00 000000 00000, 00 0000 0 00000. 00 B0 00 TXT 00000 00 0000 00000 0, 00 0 00 0000000 0000000 TXT 000000 00 0000 000000 00000. 00 D0 0 0 000000. 00 E0 00 0000 000000 0000 0000 0000, 00 0000000 00000 000000 000000 000000 00 0000 00 0 00000. 00 C0 00 00 0000 0000 0

□□□□. □□□□□ DNS, □□□□ DNS □□□□ □□□□ □□ □□, □□□□ □□□□ □□ □□(XSIAM□ □□ □□ □□), □□□□□□ □ □□ □□(□□□□ □□□□ □□□), □□ □□ DNS □□□□ □□□□ □□□□ □□ □□, □□ □□ □□ □□ □□□□□ □□□ □□ □□□□. □□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□ □□□ □□ □□ □□ □□□□.

NEW QUESTION: 33

□□□□ □□ □□ □□□□ □□□□ □□□ □□□□□□□□□ Cortex XSIAM□□ PCAP □□□ □□□□ □□□□ □□□□ □□□. □□□□ PCAP □□□□ □□□ □□□ □□ □□□□□, □ □□□ □□□ □□□ VM□ □□□ □□ □□□ □□□□ □□□□□ □□□□□ □□□□. PCAP □□ □□□□ VM□ □□ □□□□□ □□□□□ □□□□ □, □□ □□ □□□ VM□ PCAP □□□□ □□□ □□□□□ □□□□□ □□□□ □□ □□ □□□ □□ □□ □□ □□□□□□□?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 34

□□ □□□ Palo Alto Networks XSIAM□ □□□□ □□□□ □□□ □□□□□. □□ A□ □□□ □□ □□□□ □□ □□ □□□ □□□□□, □□ B□ □□□ □□□□ □□□□(AWS)□ □□□□ □. □□ A□ □□□ XSIAM□ □□ □□□ □□□ 70%□ □□ □□□ 80%□ □□□ □□□ □□ □□, □□ B□ □□ □□ □□ □□□ □□□ □□ □□□ □□□ □□□□□. □□□□ □□ □□□ □ □□ □□ □□□□□ □□□□□ □□□. □ □□□□□ □□ □□ XSIAM □□ □□□□ □□ □□□□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□ □□□ □□□□□?

- A. □□ A□ □□ B □□□ □□□□ □□ WAN □□□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□.
- B. □□□ □□□ □□□ □ □□□□ □□□ □□ □□ A□ □□□□□ □□□□□ AWS S3□ □ □□□□ □□□□□.
- C. □□ A□ AWS □□ B □□□ □□ □□□ □□□□ □□(□: AWS Direct Connect □□ □□ □□□ □□□)□ □□□□□□□□ □□ □ □□ □□□ □□□□□ □□□□ □□□□□□.
- D. □□□ □□ □□□□ □□□□ □□ □□ A□ □□ B □□□ □□□ □□ □□□□ □□(CPU, RAM, □□□□)□ □□□□□.
- E. □□ □ □□ □□ □□□ □□□ □□□ □□ □□ □ □□□ □□ □□ □□□□ □□□□□□□ □□ □□□.

Answer: ([SHOW ANSWER](#))

□□ □□, □□ □□□ □□ □ □□ □□ □□ □□ □□ □□□□□ □□□□ □□□ □ □□, □□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□ □□□□□. AWS Direct Connect(C) □ □□ □□ □□□ □□□ □□□ □□ □ □□ □□ □□□ □□ □□□□ □□□□ □ □□□□

□, □□ □□□ □□□□ XSIAM□ □□ □□□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□. WAN □□□(A)□ □□□ □ □ □□□, □□□□□ □□ □□□□ □□ □□□ □□□□□□. S3 □□□(B)□ □□□ □□□ □□ □□□□□ □□ □□□□. □□□ □□□□ □(D)□ □□□□□□ □□ □□ □□□ □□ □□□ □□ □ □□□ □□ □□□ □□□□□. □□ □□/□□ □□□□□□(E)□ □□□□ □□□ □ □□□ □ □ □□□, □□ □□□□ □□□ □□ □□□□□□.

NEW QUESTION: 35

XSIAM □□□□□ '□□□□ □□□□ □□ IP □□□□ □□□□ □□□ □□□□ □□□□□ □□□ □□'□ □□□□ □□□ □□□□ □□□ □□□□ □□□. □ □□□ '□□□□ □□□'□ □□ □□ □□, SharePoint □□□ □□ □□□□□□□ □□□□ □□□ □ □□□ □□ □□□□ □□□. □□, '□□□□ □□□□ □□ IP □□'□ □ □□□□□□ □□ 30□ □□ □□□□ □□□□ □□□□. □ □□ □□□ □□□□ □□□□ □ □□□□ XSIAM □□□□ □□ □□□ □□□□ □□?

- A. '□□□□ □□ IP'□ □□ □□ IP □□ □□□□□ □□ □ □□□ □□□ □□ □□□ □□ □□ □□ 'OR' □□ □□.
- B. □□□ □□□ □□/□□□ □□ '□□□□ □□'□ XSIAM□ '□□ □□□' □□ '□□ □□□'□ □□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□□ IP □□□ □□□□, □□□ □□□ □□□ □□□□ □□□□□□.
- C. □□ □□ □□ □□□ □□□□□. □□□ □□□ □□□□ □□□, □□□ □ □□□□ IP □□ □□□□ □□□ □□□ □□□□□.
- D. □□ IP □□ □□□□□ □□□□□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□ □□□.
- E. □□ □□□ IP□□ □□□ □□□□ □□□□□ □□ □□□□ □□ □□□ □□ 24□□ □□ □□□□ □□□□ '□□ □□'□ □□□□.

Answer: B (LEAVE A REPLY)

□□ B□ □□ □□□□ □□ □□□□□□. '□□□□ □□'□ □□ '□□□□ □□□'□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□□ □ □□□□. XSIAM□ '□□ □□□' □□ '□□ □□□'□ □□□ IP □□□ □□□ □□□□ □□□ □□□ □□□□□, '□□□□ □□□□ □□ IP □□'□ □□ □□ □□□□ □ □□□ □□□ □□□□□ □□□□□□□□□□. □□□ □□□ □□□ □□□□□ □□ □□ □□□□ □□□□□. □□ A□ □□□□ □□□□ □□□□□. □□ C□ □□□ □□□ □□□□. □□ D□ E□ □□□ □□□□□.

NEW QUESTION: 36

Cortex XSIAM□ Kubernetes □□□ □□ □□□□□ □□□ □□□□□?

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 37

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

- A. XSIAM uses CDL (Cortex Data Lake) for data storage.
- B. XSIAM uses XAE (XSIAM Analytics Engine) for data processing.
- C. XSIAM uses XAPI (XSIAM API) for data integration.
- D. XSIAM uses SOAR (Security Orchestration, Automation, and Response) for incident response.
- E. XSIAM uses XDR (XSIAM Data Repository) for data storage.

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 38

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

- A. XSIAM uses XDR (XSIAM Data Repository) for data storage.
- B. XSIAM uses XAE (XSIAM Analytics Engine) for data processing.
- C. XSIAM uses XAPI (XSIAM API) for data integration.
- D. XSIAM uses SOAR (Security Orchestration, Automation, and Response) for incident response.
- E. XSIAM uses CDL (Cortex Data Lake) for data storage.

Answer: (SHOW ANSWER)

XDR can collect data from 'remote log files' and process them into a single view (B) and generate alerts. Additionally, XSIAM can integrate with Cortex XDR and API to provide a unified view (C) of all data. XSIAM can also integrate with other security tools (A) and provide a single view of all data. XSIAM can also integrate with other security tools (D) and provide a single view of all data. XSIAM can also integrate with other security tools (E) and provide a single view of all data.

NEW QUESTION: 39

XSIAM can provide a single view of all data, including logs, alerts, and events. XSIAM can also integrate with other security tools and provide a single view of all data. XSIAM can also integrate with other security tools and provide a single view of all data. XSIAM can also integrate with other security tools and provide a single view of all data.

- A. XSIAM can provide a single view of all data, including logs, alerts, and events.
- B. XSIAM can provide a single view of all data, including logs, alerts, and events. XSIAM can also integrate with other security tools and provide a single view of all data.
- C. XSIAM can provide a single view of all data, including logs, alerts, and events.
- D. XSIAM can provide a single view of all data, including logs, alerts, and events.
- E. SOC can provide a single view of all data, including logs, alerts, and events.

Answer: B (LEAVE A REPLY)

XSIAM can provide a single view of all data, including logs, alerts, and events. XSIAM can also integrate with other security tools and provide a single view of all data. XSIAM can also integrate with other security tools and provide a single view of all data. XSIAM can also integrate with other security tools and provide a single view of all data.

NEW QUESTION: 40

XSIAM can provide a single view of all data, including logs, alerts, and events. XSIAM can also integrate with other security tools and provide a single view of all data. XSIAM can also integrate with other security tools and provide a single view of all data. XSIAM can also integrate with other security tools and provide a single view of all data.

Which of the following is a valid C2 channel for XSIAM? (Select all that apply)

- A. A
- B. B
- C. C
- D. D
- E. E

Answer: C (LEAVE A REPLY)

Which of the following is a valid C2 channel for XSIAM? (Select all that apply) A) B) C) D) E) XSIAM is a cloud-based platform for managing and monitoring IoT devices. It uses a variety of channels to communicate with devices, including cellular, Wi-Fi, and Bluetooth. The C2 channel is the primary channel used for command and control. The valid C2 channels are C) and D).

NEW QUESTION: 41

Which of the following is a valid channel for XSIAM? (Select all that apply) A) B) C) D) E) XSIAM is a cloud-based platform for managing and monitoring IoT devices. It uses a variety of channels to communicate with devices, including cellular, Wi-Fi, and Bluetooth. The valid channels are B) and C).

- A. A
- B. B
- C. C
- D. D
- E. E

Answer: B (LEAVE A REPLY)

Which of the following is a valid channel for XSIAM? (Select all that apply) A) B) C) D) E) XSIAM is a cloud-based platform for managing and monitoring IoT devices. It uses a variety of channels to communicate with devices, including cellular, Wi-Fi, and Bluetooth. The valid channels are B) and C).

□ □□□□ □□□ □□□□ □□□□□ □ □□□ □□□ □ □□□ □□□□(CPU, RAM, I/O □ □)□ □□□□□. '□□□ □□□(noisy neighbor)'□□ □□□ □□ □□□□ □□□□ □□□, □ □□ HCI □□ □ □□□ □□□ □□ □□□ □ □□□□. □□□□(C)□ □□□□ □□□□□, XSIAM □□□ □□ □□□ □□□□ □□□ □□□ HCI□ □□□ □□ □□□□ □□□□□. GPU(D)□ □□□□ XSIAM □□ □□□□ □□□□ □□□ □□□□. □□ □□□□/□□□□ □□ □□ XSIAM□ □□ □□ □□□(E)□□ □□□□ □□□□ MSSP □□□□ □□ □□□ □□□ □□□□.

NEW QUESTION: 42

□□ □□□ Cortex XSIAM □□□ □ □□□□□ □□□□ □□□□□ □□□□□, □□ □□□ '□ □□□ □□ □□: □□□ □□□ □□ □□'□□ □□□□ □□□□□. □□□ □□□□ □□□□ □□ □□□□ □□□□□ □□□□□. □□ □□ □□, XSIAM □□□□ □□ □□ □□□□ □□ □□□□□□, XSIAM □□ □□□ □□□□ □ □□ □□□ □□□ □□□ □□□ □□□□□□. □□ □ □□ □□ □□ □□□ □□□□, □□□ □□□□□□□□□?

- A. XSIAM □□□ □□ □□□ □□ □□□□□ □□ □ □□□□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□. □□□ NTP□ □□ □□□□□□□.
- B. □□□ □□□□□ □□ XSIAM □□□□ □□□□ □□□□ □□□□□□□□□, □□ □□□ XSIAM □□(□□ □ □□□□)□ □ □□□ □□□ □□□□ □□□□. □□ □□□□□ □□ □ □□□ □□□□ □ □□□□. □□ □□□ □□□□ □□ □□□□□ □□ □□□□□□□ □□ □□□ □□□□ □, □□ □□□ □□□□□ XSIAM □□□ □□□□□ □□ □□□ □□□ □□ □ □□□□ □□□□.
- C. □ □□□□□□ XSIAM □□ □□ □□ 443 □□□ □□□□ □□□□ □□□□. □□□ □□ □ □□□□□.
- D. XSIAM □□□ □□□ □□□ □□□□ □ □□□□ □□□ □□□ □ □□□□. □□□ □□□ □□□ □□□□□.
- E. □□ □□□□□ □□□□□ XSIAM □□□ □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)

□□□ □□ □□□ '□□□□ □□□□ □□□□□□ □□□□ □□□□□ □□□□□', '□□ □□ □' □□□□□□□ '□□□□ □□ □□□□□' □ □□□ □□□ □□ □□□ □□□□□ □□□□. □□ □□□ □□□□□ □□□ □□□ □□□□ □□□□ □□□□□. Cortex XSIAM □□□□ □□□□□□□ □□□□ □□□ □ □□□ □□□□ □□□□ □□□□□ □ □□□□. □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □ □□□, □ □□□□ □□□ □ □□□□□ □□ □□ □□ □□□□□□ □□□□ □ □□□ □□ □□□ □□ □□□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□□□. XSIAM □□ □□□ □ □□□ □□□□ □□□□□ □□□□ □ □ □□□□. □□ A □ □□□□ □□□ □ □□□□□□□ □□□ □□ □□□□ □□□□. □□ C□ □ □□□□□□ □□□ □□ □□□□□ □□□ □□□□. □□ D□ □□ □□(□: □□□ □□ □)□ □□□□□. □□ E□ □□□□ □□□ □□□□□ □□ □□□ □□□□□ □□□□□ □□□□ □□□ □ □□□□ □□□□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□□□ □□□□ □□□ □□□

Which of the following is a valid XSIAM URL? (Select two.)

NEW QUESTION: 43

XSIAM is a REST API that runs on Linux. Which of the following are valid XSIAM URLs? (Select two.)

- A. `https://us.xdr.paloaltonetworks.com/xdr/api/v1/production_linux`
- B. `https://production_linux.xdr.paloaltonetworks.com/xdr/api/v1`
- C. `https://us.xdr.paloaltonetworks.com/xdr/api/v1/production_linux`
- D. `https://us.xdr.paloaltonetworks.com/xdr/api/v1/production_linux`
- E. `https://us.xdr.paloaltonetworks.com/xdr/api/v1/production_linux`

Answer: (SHOW ANSWER)

Correct answers: C, D. XSIAM is a REST API that runs on Linux. The valid XSIAM URLs are `https://us.xdr.paloaltonetworks.com/xdr/api/v1/production_linux` and `https://us.xdr.paloaltonetworks.com/xdr/api/v1/production_linux`. The other options are invalid because they do not use the correct domain name or path.

NEW QUESTION: 44

XSIAM is a REST API that runs on Linux. Which of the following are valid XSIAM JSON objects? (Select two.)

'event_data' field in the JSON object returned by XSIAM? `jq -r '.event_data'`

- A. Use the `jq` command `jq -r '.event_data'` to extract the value of the `event_data` field from the JSON object.
- B. Use the `jq` command `jq -r '.event_data'` to extract the value of the `event_data` field from the JSON object. Alternatively, you can use the `jq` command `jq -r 'json_extract(event_data)'` to extract the value of the `event_data` field from the JSON object.
- C. Use the `jq` command `jq -r '.event_data'` to extract the value of the `event_data` field from the JSON object. Alternatively, you can use the `jq` command `jq -r 'json_extract(event_data)'` to extract the value of the `event_data` field from the JSON object.
- D. XSIAM uses the `jq` command `jq -r '.event_data'` to extract the value of the `event_data` field from the JSON object.
- E. 'event_data' is a field in the JSON object returned by XSIAM.

Answer: B (LEAVE A REPLY)

The correct answer is B. The `jq` command `jq -r '.event_data'` is used to extract the value of the `event_data` field from the JSON object. Option A is incorrect because it does not use the `jq` command. Option C is incorrect because it does not use the `jq` command. Option D is incorrect because XSIAM does not use the `jq` command. Option E is incorrect because 'event_data' is a field in the JSON object returned by XSIAM.

NEW QUESTION: 45

Cortex XSIAM uses various protocols to communicate with external systems. Which protocol is used by XSIAM to communicate with AWS S3 for log storage? XSIAM uses the following protocols to communicate with external systems: HTTP (80), HTTPS (443), Syslog, API, and SSH (22). Which protocol is used by XSIAM to communicate with AWS S3 for log storage?

- A. XSIAM uses HTTP (80) to communicate with AWS S3 for log storage.
- B. XSIAM uses HTTPS (443) to communicate with AWS S3 for log storage.
- C. XSIAM uses Syslog to communicate with AWS S3 for log storage.
- D. XSIAM uses SSH (22) to communicate with AWS S3 for log storage.
- E. XSIAM uses API to communicate with AWS S3 for log storage.

Answer: (SHOW ANSWER)

Cortex XSIAM uses various protocols to communicate with external systems. Which protocol is used by XSIAM to communicate with AWS S3 for log storage? XSIAM uses the following protocols to communicate with external systems: HTTP (80), HTTPS (443), Syslog, API, and SSH (22). XSIAM uses HTTPS (443) to communicate with AWS S3 for log storage.

Q. Which of the following protocols does XSIAM support? (Select all that apply.)
A. HTTP
B. HTTPS
C. SSH
D. ICMP
E. REST API

NEW QUESTION: 46

XSIAM supports REST API. Which of the following protocols does XSIAM support? (Select all that apply.)
A. HTTP
B. HTTPS
C. SSH
D. ICMP
E. REST API

- A. HTTP is supported, Python is supported API is supported, 'REST API' is supported.
- B. 'REST API' is supported, 'HTTP API' is supported, API is supported, 'SSH' is supported.
- C. 'REST API' is supported XSIAM supports REST API is supported.
- D. 'VirusTotal' is supported.
- E. REST API is supported.

Answer: (SHOW ANSWER)

XSIAM supports REST API. Which of the following protocols does XSIAM support? (Select all that apply.)
A. HTTP
B. HTTPS
C. SSH
D. ICMP
E. REST API

XSIAM-Engineer is a dump of Palo Alto Networks XSIAM-Engineer. DumpTop is a dump of XSIAM-Engineer. DumpTop XSIAM-Engineer is a dump of XSIAM-Engineer. DumpTop XSIAM-Engineer is a dump of XSIAM-Engineer. <https://www.dumptop.com/Palo-Alto-Networks/XSIAM-Engineer-dump.html> (436 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

Which of the following is the correct SIEM search query to identify critical exploit attempts for CVE-2023-XYZ, where the process name is 'diag_tool.exe' and the user name is 'admin_user'?

- A. Palo Alto Networks SIEM search query: 'Critical_Exploit_Attempt_CVE-2023-XYZ' AND 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user''
- B. Palo Alto Networks SIEM search query: 'Critical_Exploit_Attempt_CVE-2023-XYZ' AND 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user''
- C. Palo Alto Networks SIEM search query: 'alert_name = AND 'destination_port= '8080'' AND 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user''
- D. Palo Alto Networks SIEM search query: 'Critical_Exploit_Attempt_CVE-2023-XYZ' AND 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user''
- E. Palo Alto Networks SIEM search query: 'diagnostic_servers' AND 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user'' AND 'Critical_Exploit_Attempt_CVE-2023-XYZ' AND 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user'' AND XSOAR

Answer: B (LEAVE A REPLY)

Option B is the correct SIEM search query. It uses the AND operator to filter for critical exploit attempts for CVE-2023-XYZ, where the process name is 'diag_tool.exe' and the user name is 'admin_user'. Option A is incorrect because it uses single quotes around the process name and user name. Option C is incorrect because it uses AND incorrectly. Option D is incorrect because it uses AND incorrectly. Option E is incorrect because it includes XSOAR, which is not a SIEM search query.

NEW QUESTION: 49

Which of the following is the correct SIEM search query to identify authentication failures for a specific IP address, where the source IP is '192.168.1.1' and the country is 'USA'?

- A. Palo Alto Networks SIEM search query: 'source_ip = '192.168.1.1' AND 'country = 'USA' AND 'username = 'admin' AND 'Authentication = 'failure''
- B. Palo Alto Networks SIEM search query: 'source_ip = '192.168.1.1' AND 'country = 'USA' AND 'Authentication = 'failure''

C. XSIAM 'source_ip' field is not populated. The field is empty. 'authentication_status' is 'failure'. 'source_ip' field is empty. 'Authentication' field is empty.

D. 'source_ip' 'country' 'city' fields are populated. The fields contain values. 'source_ip' 'country' 'city' fields are populated.

E. 'source_ip' field is populated with IP address. The field contains a valid IP address. 'source_ip' field is populated with IP address. The field contains a valid IP address.

Answer: (SHOW ANSWER)

The question asks for the correct field values. Option D is correct because 'source_ip', 'country', and 'city' are populated. Option A is incorrect because 'source_ip' is empty. Option B is incorrect because 'authentication_status' is 'failure'. Option C is incorrect because 'Authentication' is empty. Option E is incorrect because 'source_ip' is not a valid IP address.

NEW QUESTION: 50

Which of the following methods is used to set the incident fields?

- A. !setIncidentFields
- B. !setParentIncidentFields
- C. !setParentIncidentContext
- D. !updateParentIncidentFields

Answer: A (LEAVE A REPLY)

!setIncidentFields is used to set the incident fields. The method is used to set the incident fields.

NEW QUESTION: 51

XSIAM은 어떤 SOAR 플랫폼과 통합될 수 있는가? 다음 중 옳지 않은 것은 무엇인가?

- A. XSIAM은 Python을 사용하여 API를 호출할 수 있다.
- B. XSIAM은 Python의 'time' 모듈을 사용하여 실행 시간을 측정할 수 있다.
- C. XSIAM은 REST API를 사용하여 외부 시스템과 통신할 수 있다.
- D. XSIAM은 CPU 사용량을 모니터링할 수 있다.
- E. XSIAM은 PDF 파일을 생성할 수 있다.

Answer: A,B (LEAVE A REPLY)

XSIAM은 Python을 사용하여 API를 호출할 수 있다. Python의 'time' 모듈(B)은 실행 시간을 측정할 수 있다. C, D, E는 XSIAM의 기능이다. A와 B는 옳지 않은 설명이다.

NEW QUESTION: 52

XSIAM은 SOAR 플랫폼과 통합될 수 있는가? 다음 중 옳지 않은 것은 무엇인가?

- A. XSIAM은 REST API를 사용하여 외부 시스템과 통신할 수 있다.
- B. XSIAM은 Python을 사용하여 API를 호출할 수 있다.
- C. XSIAM은 REST API(예: ServiceNow, HR 시스템)를 사용하여 외부 시스템과 통신할 수 있다.
- D. XSIAM은 사용자 인터페이스(GUI)를 제공할 수 있다.
- E. XSIAM은 PDF 파일을 생성할 수 있다.

Answer: (SHOW ANSWER)

SOAR은 REST API를 사용하여 외부 시스템과 통신할 수 있다. Python을 사용하여 API를 호출할 수 있다. XSIAM은 REST API(예: ServiceNow, HR 시스템)를 사용하여 외부 시스템과 통신할 수 있다. XSIAM은 사용자 인터페이스(GUI)를 제공할 수 있다. XSIAM은 PDF 파일을 생성할 수 있다.

NEW QUESTION: 53

Which of the following is a valid XSIAM API endpoint? XSIAM API endpoints are in the format /api/v1/resource. Which of the following is a valid XSIAM API endpoint?

- A. API endpoint /api/v1/resource is a valid XSIAM API endpoint.
- B. /api/v1/resource is a valid XSIAM API endpoint.
- C. /api/v1/resource, /api/v1/resource, /api/v1/resource is a valid XSIAM API endpoint.
- D. XSIAM API endpoint /api/v1/resource is a valid XSIAM API endpoint.
- E. /api/v1/resource API endpoint is a valid XSIAM API endpoint.

Answer: (SHOW ANSWER)

The correct answer is B. /api/v1/resource is a valid XSIAM API endpoint. XSIAM API endpoints are in the format /api/v1/resource. The other options are not valid XSIAM API endpoints. Option A is missing the /api/v1 prefix. Option C is missing the /api/v1 prefix and has a trailing comma. Option D is missing the /api/v1 prefix. Option E is missing the /api/v1 prefix and has a trailing comma.

NEW QUESTION: 54

Which of the following is a valid XSIAM API endpoint? XSIAM API endpoints are in the format /api/v1/resource. Which of the following is a valid XSIAM API endpoint?

- A. XSIAM API endpoint /api/v1/resource (RBAC) is a valid XSIAM API endpoint.
- B. /api/v1/resource is a valid XSIAM API endpoint.
- C. /api/v1/resource, /api/v1/resource, /api/v1/resource is a valid XSIAM API endpoint.
- D. XSIAM API endpoint /api/v1/resource is a valid XSIAM API endpoint.
- E. /api/v1/resource API endpoint is a valid XSIAM API endpoint.

Answer: (SHOW ANSWER)

□□ □□ □□ □□□□□. A□ D□ □□ □□□□ □□ □□□□ □□ □□□□□. □□ A: XSIAM□ RBAC□ □□□ □□ □□□ □ □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□. □□□ □ □□ □□□ '□□□□' □□□□□ □□□ □□ □□□ □□□□□□ □□ □□□ □□□ □ □□□□. □□ □□□□ □□ □□□□□. □□ D: XSIAM(XSOAR)□ □□ □□ □ □□□ □□ □□□□□□ □□□□ □□□□□□. '□□□□' □□□□ □□□□□□□ □□□ □□ □□□□ □ □□□ □□□ □□ □□□ □ □□□□ □□ □ □□□□. □□ □□ □□□ □ □□ □□□□□ □□□ □ □□□□□□□□□□ □□ □□ □ □□□ □ □□□. □□ □□□□ □□□□□□□□□□□ □□ □□ □ □□□ □ □□□. □□ □□□□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□ □□□□□. □□ B□ □□□ □□□□□ □□ □□ □□□ □□□□ □□□, □□□ □□□□ □□□ □□□ □ □□ □□□ ID□ □□□□□. □□ C□ □□ □□ □□□□ □□□□□ XSIAM □□□ □□□ □□ □□ □□□□. □□ E□ □□□□ □□□□ □□□ □□□□ □□□□□ □□ XSIAM □□□□□ □□□□ □□/□□□□/□□□□ □□□□ □□ □□□□□□□□.

NEW QUESTION: 55

□ □□ □□□ □□(CIO)□ □□□□□ IT□ □□□ □□ XSIAM□□ OT(□□ □□) □□ □□□ □□□□ □□□□ □□□□. OT □□□ SCADA □□□, PLC, HMI□ □□□□ □□□, □□□ □ □□□ □□ □□ □□□□□ □□□□□. OT □□ □□ □□□ XSIAM□ □□□□ □ □□ □□ □□□ □□□□, IT□ OT □□ □□ □□□ □□□□ □ □□ □□□ XSIAM □□□□ □□ □□ □□ □□□ □□□□□?

- A. □□: XSIAM □□□□□ OT □□□ □□□ □ □□□□. □□ □□□□□ □□ □□□ □□□ □□. □□ □□: □□□□ □□ OT □□□□ □□(□: Claroty, Nozomi Networks)□ □□□□ □□ OT □□□□□ IT □□□□□ □□(□: NetFlow, syslog)□□ □□□ □ XSIAM □□□□ □□□□ □□□□.
- B. □□: OT □□□ IT □□□ □□□□□ □□□□ □□□□. □□ □□: OT □□□□ USB □□ □□□ □□□ □□□ IT □□□□□ XSIAM □□□ □□□□ □□□□□ □□□□ □□□□□.
- C. □□: OT □□□□ □□□ □□□□ □□ □□□□□. □□ □□: OT □□□ □□□ □□□ □ □□□ □□□□□ XSIAM□ □□□□□.
- D. □□: XSIAM□ AI/ML □□□ OT □□□□ □□□□ □□□□ □□□□□. □□ □□: OT □□ □□ □□ □ □□ □□□ □□ □□□ XSIAM □□ □□ □□□ □□□□□.
- E. □□: XSIAM□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□□□. □□ □□: □□ OT □□□□□□ XSIAM □□□□□□ □□□□ □□ □□□□□ VPN □□□ □□□□□.

Answer: A (LEAVE A REPLY)

XSIAM□ □□ □□ □□ □□□□□ OT □□□ □□□□ □□ □□□ □□□ □□□□□. □□□ □□ OT □□□ □□□□□ □□ □□□□ □□ □□ □□□□□□ □□□□□. □□ □□□□□ IT □□ □□□ □□□□□ □□□□ □□□□. □□ □□□□□ □□□□ □□□ OT □□□□ □ □□ OT □□□□□ □□□□ □□□(□: Claroty, Nozomi Networks, Dragos)□ □□□□ □□□ □. □□□ □□□□□ OT □□□□□ □□□□□□ □□□□□□□, □□ □□□□□ □□□□□, □□ □ □□ □□□ □ □□ □□ □□□ □ □□□□ □□ □□□□ □□ □□□□ □□ IT □□(□: syslog, NetFlow/IPFIX, API □□)□□ □□□ □ □□□□. □□□ □□□□□ □□□□ XSIAM □□□ □□ □□ □□ □□□ □ □□□, OT □□□ □□□□□□ □□□□□ IT□ OT □□ □□□ □□□ □□□

`alert.count > 10` `alert.count` `15(10 + 5)`. `50 + 30 = 80.4`. `2: 'alert.detection_rule_id = 'app_crash_detection' AND alert.app_name in ('ERP', 'CRM') alert.app_name = 'ERP'(1)` `xl .5` `'app_crash_detection'` `'Crash'` `1` `1.5 = 45` `50 + 45 = 95` `95` `120` `(100)`, `95`.

NEW QUESTION: 58

Windows `Process.Name = 'seclogon.exe'` `'psexec.exe'` `BIOC` `IT` `(false positive)` `XQL`?

- A.
- B.
- C.
- {<>}:
 - D.

Answer: B (LEAVE A REPLY)

B `XQL`. A `seclogon.exe` `psexec.exe` `seclogon.exe` `D` `'pattern'` `'seclogon.exe'` `'psexec.exe'` `(100)`, `(100)`, `(200)`. `'where stage_1 - Process.Reputation != 'trusted' and stage_2.Process.Reputation != 'trusted''`

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

NEW QUESTION: 61

XSIAM □□□□ □□□□ □□□□ □□□□ □ □ □□ □ □ □□ □□ □□ □□□□ □□□□ □□□□ □□. □□□□□□ □ □ S3 □□ □□□□ □ □ □□□□ □ □ □□□□ □□□□. □□ □ □ □□□ □ □ □□□□ □ □ □□□□ □ □ □□ □ □ □□ □ □□□. □□□□ □□ API □□□□ □□□□ □□ □ □ □□□ □ □ □ □ □ □□□□□ □ □ □□ □□ □□□□ □□□□ □□□□ □□ □ □ □□□?

- A. '□□ □ □ □□□' □□ □□□□ S3 □ □ □ □ □ □ □□ □□□□ □□, '□□' □□□□ '□□□' □□□ □□□□ □□□□□.
- B. □□□ □ □ Lambda/Azure Function API Gateway □□□□□□ □□□□ '□□ API □□' □ □ □ □□□□. □ □□□□□□ □□□ □□□□ S3 □ □ □□ □□□□ □ □ □□ □□□□ □.
- C. □ □ □□ □□ □ □ □ □ XQL □□□□ □□□□ S3 □□ □ □ □□□□ 'XQL □ □ □□' □□□ □□□□□.
- D. XSIAM □ □ '□□ □□' □ □ □□ □□□□ □ □ □□□□ □ □ □□□□ □□□□□ □ □ '□□□' □□□ □□□□ '□□ □□' □ □□□□.
- E. '□□ □□' □□□ □□□□ □ □ □□□□ □□□ S3 □ □ □□ □ □ □□□□ □□□□□ □□□.

Answer: (SHOW ANSWER)

□□□ □ □ □□□□□(A) □□□ □□□□□□ □ □ □□□□□ □□□□ □ □ □□□□□. XQL(C) □ □□ □□□□ □□ □ □ □□ □□ □ □ □□ □ □ S3 □□□ □ □ □□□□ □□□□. '□□ □□'(D) □ □□□□□□ □□□□ □ □ □□□□□, '□□ □□' '□□□□ □ □□□' □□ □□□□ □□□□□ □□□□ □□ □ □ □□ □□□□ □ □ □□ □ □ □□ □ □ □□ □ □ □□ □ □ □□ □ □ □□□□. '□□ □□'(E) □ □□□□ □□□□□□□. □□□ □□□ □ □ □□□□ □□(B) □ □□□□ □ □ □ □□□□□ □ □ □□ □ □ □□□□□. □□□□□ □ □□□ □ □ □ □ □□□ □□□□ □□□□ □□□ S3 □□□□ □ □ □□□□ □□□□□ □□□□ □□□ □□□□ □□□ □□□□□. □ □ □□□□ □□□ □□□ □□□□□.

XSIAM-Engineer □□ □□□ □□□□□ □ □ DumpTop □ □ □□□ □□□ XSIAM-Engineer □□! DumpTop □ □ □ **XSIAM-Engineer** □□ □□□ □□□□□□, DumpTop XSIAM-Engineer □ □ □□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □ □ □ □ □ DumpTop XSIAM-Engineer □□□ □□□□□. <https://www.dumptop.com/Palo-Alto-Networks/XSIAM-Engineer-dump.html> (436 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 62

XSIAM endpoint_status_logs is_signature_current is SQL injection?

- A.
B.
C.

{<>}:

- D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 63

XSIAM endpoint_status_logs is_signature_current is SQL injection?

- A.
B.
C.
D.
E.

Answer: C (LEAVE A REPLY)

XSIAM endpoint_status_logs is_signature_current is SQL injection?

□ □□□ □□□. □□ B□ □□□□□□ □□□ □□ □□□□ □□□ □□□□ □□, □□□ □ □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□. □□ D□ □□□ □□ □□□ □ □□□□ □□□ □□ □□□ □□□ □ □□□□. □□ E□ □□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□ ID □□□ □□ □□ □□□□□.

NEW QUESTION: 64

□□□□□ □□□ □□ □□ Cortex XSIAM □□□ A□□ Cortex XSIAM □□□ B□ Cortex XDR □□□□□ □□□□□□□□□ □□□.

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

XDR □□□□ <-> □□□ A <-> XSIAM □□□ A

XDR □□□□ <-> □□□ B <-> XSIAM □□□ B

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

- A. □□□ B□ □□□ □□□ C□ □□□□ Cortex XSIAM □□□ A□ □□□□□.
- B. □□□□ □□□ □□□ C□ □□□□ Cortex XSIAM □□□ B□ □□□□□.
- C. □□ Broker A□ Cortex XSIAM □□□ B□ □□□□□.
- D. □□□□ □□ □□□□□□ □□□□ □□□□ □ □□□ C□ □□□□□.

Answer: B,C (LEAVE A REPLY)

□□□□ □□ XDR □□□□□ □□□ A□□ □□□ B□ □□□□□□□□□□ □□□□□ □□□ □□□□ □□ □□□ B□ □□□ □□□ □□□ C□ □□□□ □□, □□□□□□ □□ □□ □ □□□□ □□ □□□ □□□□ □□□ □ □□□ □□□ A□ □□□ B□ □□□□ □□□.

NEW QUESTION: 65

□□□ XSIAM □□ □□□□ □□□□ □□□ □□□□ NGFW□□ □□ □□ □□□ □□□□□ □□□□ □□□□□ □□□ Palo Alto Networks NGFW□ □□ □□□□ □□□ □□(□ □□)□ □ □□□□. XSIAM □□□□ □ □□□ □□ □□□□ □□□□□, □□ □□□□ □□□ □□□ □. □□ □□ □□□ □□□ □□□□□. □□ □ XSIAM □□□ □□ □□□□□ □□ □□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□ □□□□□?

- A. XSIAM □□□□ □□□ CPU□ □□□□ □□□□□. □□ □□□□ □□□□□□□, □□ □□ □□□ □□ □□□ □□ □□□□.
- B. XSIAM Collector□ 'collector.log' □ 'pipeline.log'□ □□□□ □□ □□, □□□□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□□. □□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□□.
- C. □□□ □□ □□□ □□□ □□ □□ □□□ □□ □□ □□ □□ □□□ □□□ □□□□□ □□□□□□ □□□ □□□□□ □□□□□. □□□□ □□ □□□ □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □ □□□ □□□, □□□□ □□□ □□□ □□□□□.
- D. XSIAM Data Lake□ □□□ I/O □□□ □□ □□□ □□□□□. □□□ □□□□□□, □□□ □ □□ □□ □□ (□□) □□ □□ □ □□ □□ □□□ □□□□□.
- E. □□□ □□□□ □□ □□ XSIAM □□□□ □□□□□. □□ □□ □□□ □□□□ □□ □□ □□ □□ □□ □□□ □□□ □□ □□□□□□.

Answer: B (LEAVE A REPLY)

... .. , **B**
... .. (, ,) **A**
... .. . **C** **D**
... .. .

NEW QUESTION: 66

- A. A
- B. B
- C. C
- D. D
- E. E

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

NEW QUESTION: 67

- A. A
- B. B
- C. C
- D. D
- E. E

Answer: ([SHOW ANSWER](#))

B 1: **XSIAM** 2: 3: **C2** (false positive)

NEW QUESTION: 68

... Palo Alto Networks **XSIAM**

- A. **XSIAM** **TPM 2.0**(... ..)

- B. XSIAM (Intel SGX, AMD SEV).
- C. ,
- D. 'Chain of Custody' (D)
- E. (HSM) FIPS 140-2 3

Answer: A,C,D,E (LEAVE A REPLY)

TPM 2.0(A), (Chain of Custody) (D) HSM(E) FIPS 140-2 3 (B)

NEW QUESTION: 69

3 Cortex XSIAM IP SBAC

3 IP SBAC

- A. "EG:Building3" IP SBAC
- B. "EG:Building3" SBAC
- C. "EG:Building3" SBAC
- D. "EG:Building3" SBAC

Answer: (SHOW ANSWER)

Building 3 IP SBAC EG:Building3 Building 3 IP SBAC

NEW QUESTION: 70

□□□, □□□□ □□ □□□□ □□□ □□□ □□ □□ □□□□□□. □□ E□ XSIAM□ □□□□ □□□□□ □□□□ □ □□□□ □□ □□□□□□□□.

NEW QUESTION: 74

XSIAM □□□□□ □□□ □□□□ □□□ □□□□ □□□ □□ □□□□□□ □□□□ □□□ □ Jira □□□ □□□□ □□□ □□□ □□□□□ □□□ □□□ □□□□□. □ □□□□□ □□ □□ □ □□ □□□ XSIAM □□□ □□ □□□ □□□ □□□□□, Jira □□ □□□□ □□□ □ □□ □□□□□□?

- A. □□ □□ -> □□□□ □□ -> □□□□(Cortex XDR □□ □□) -> □□□□ □□ □□(Jira□)
- B. □□□□ □□□□ -> □□ □□ □□ □□□□(Jira □□ □□) -> □□ Cortex XDR □□
- C. □□ □□ □□ □□ □□ □□□ □□ □□□□(Cortex XDR □□ □ Jira □□ □□)
- D. □□□□ □□ □□ □□□ □□□□(□□□□ □□ □□) □□ □□□□(□□ □ Jira□)
- E. □□ □□ -> □□□□(□□ □ Jira □□□□ □□ □□□ □□ □□ □□)

Answer: C (LEAVE A REPLY)

□□ □□□ □□ □□ □□□□ □□□ □□ □□□ □□□ □□□ □□□□. □□ □□(□□□□ □□ □□) -> □□□□ □□(□□ □□ □□□□ □□) -> □□□□ □□(□□□□□□ □□ □□□□ □□ □□□□ □□) -> □□□□(Cortex XDR □□ □□ □ Jira □□ □□ □□□□□□□□). Jira □□□□ □□ □□□□ □□□, □□ □□□□ □□ □□□□ □□□ □ XSIAM □□□□□□ □□ □□(□: □□□□ ID, □□□□ □□ □□□, □□ □□ □□)□ Jira □□□□□□ □□□ □□□ □□ □□ □□□□ □□□□ □□□□. □□ □□□□ XSIAM □□□□ □ □□ □□□□ □□ □□□□ □□□ Jira □□ □□□ □□□□ □□□□ □□□□.

NEW QUESTION: 75

□ □□ □□□□ XSIAM□ □□□□ □□□, □□ □□ □□(□□□□) □□□ □□□□□□□ □□□. □□, □□□ XSIAM □□□ □□ □□□ □□□ □□□ □□□□ □□, □□□□□□ Delinea Secret Server PAM □□□□ □□ □□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □□□. □□ □□□ □□□ □□□□□ □□ □□□ □□□□□□□ □□□ Delinea API□ XSIAM□ □□□ □ □□□□ □□□□□. □□ □□ □□ □□□ □□□□□ □□□□ □□□□ □□□?

- A. XSIAM □□□□□ □□ □□ □□ Delinea API □□ □□ □□□□□.
- B. HashiCorp Vault□ □□ □□ □□ □□ □□□□□ □□□ API □□□□□ □□□ □□ XSIAM '□' □□ '□□'□ □□□□ XSIAM □□□□ □□ □□□□□□□.
- C. XSIAM □□□□□ □□□□□ Delinea API □□ □□ □□□ □□□□□ □□□□□.
- D. API □ □□ Delinea API □□□□□ □□ IP □□ □□□□□ □□□□□.
- E. □ □□□□ □□□ Delinea API □□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

API □□□□ □□ □□ □□□ □□□□ □□□□ □□ □□□□ □□□□□. □□□□ API □□ □□ □□□ □□ □□□□□(A) □□ □□□ □□□□□ □□□□ □(C)□ □□□□ □□ □□□□□. IP □□ □□□ □□□□□ □(D)□ □□ □□ □□ □□□ □□□□□ □□□□□ □□□□□□□□ □□□□□ □□□□□. □□ □□(E)□ □□□□□ □□□□□□□□. □□ □□□□ □□ □□□ □□ □□ □□ XSIAM □□□□□ □□ HashiCorp Vault, Azure Key Vault □□ AWS Secrets Manager□ □□

{< >}:

D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 79

XSIAM is a cloud-based SIEM solution that provides a centralized view of security events across multiple cloud environments. It integrates with various cloud providers and services to collect and analyze logs, alerts, and events. XSIAM offers a user-friendly interface for monitoring and investigating security incidents, along with advanced analytics and reporting capabilities. Which of the following is a key feature of XSIAM?

- A. XSIAM provides a centralized view of security events across multiple cloud environments.
- B. XSIAM integrates with various cloud providers and services to collect and analyze logs, alerts, and events.
- C. XSIAM offers a user-friendly interface for monitoring and investigating security incidents.
- D. XSIAM provides advanced analytics and reporting capabilities.
- E. XSIAM is a cloud-based SIEM solution that provides a centralized view of security events across multiple cloud environments.

Answer: B (LEAVE A REPLY)

XSIAM is a cloud-based SIEM solution that provides a centralized view of security events across multiple cloud environments. It integrates with various cloud providers and services to collect and analyze logs, alerts, and events. XSIAM offers a user-friendly interface for monitoring and investigating security incidents, along with advanced analytics and reporting capabilities. Which of the following is a key feature of XSIAM?

NEW QUESTION: 80

XSIAM is a cloud-based SIEM solution that provides a centralized view of security events across multiple cloud environments. It integrates with various cloud providers and services to collect and analyze logs, alerts, and events. XSIAM offers a user-friendly interface for monitoring and investigating security incidents, along with advanced analytics and reporting capabilities. Which of the following is a key feature of XSIAM?

- A. XSIAM provides a centralized view of security events across multiple cloud environments.
- B. XSIAM integrates with various cloud providers and services to collect and analyze logs, alerts, and events.
- C. XSIAM offers a user-friendly interface for monitoring and investigating security incidents.
- D. XSIAM provides advanced analytics and reporting capabilities.

□□ □□□□□. □ □□□ 'Process.Reputation 'unknown' OR Process.Reputation 'malicious'□
□ □□□□□.

D. □□□□ □□□ □□□□□□ □□□ □□□□□.

E. □□ 4444□ C2□ □□□□□□ □□ □□□□□ □□□ □□□□□.

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

□□ C□ □□ □□□□ □□□ □□□ □□□□□. □□ A□ B□ □□ □□ □□□ □ □□□, □
□□□ □ □□□, □□ C□ □□ □□□□ □□□□ □□ □□□ □□□□□. □□ C□ □□ □□
□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□□□ □□□ □□□□□ □□□□□ □
□□ □□□□ □□□□ □□□ □ □□□ □□□. □□ □□ XSIAM□ □□□ □□□□ □□□□
□□ □□ □□□□ □□□□ □□□ □□□□□□□ □□□□ □□ □□□ □□□ □□ C2 □□
□ □□□□□ □□□ □ □□□□. □□ D□ C2□ □□□□□□ □□□, □□ E□ □□□ □□□□
□ □□ □ □□□□.

NEW QUESTION: 81

□ □□□ □□□□□ □□□ □□□ □□□ □□□ VMS□ □□□□ □□□□. □ □□□ □□□
□□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□. □□ □□□□□
□□□□ SSL □□□ □□□□ □□ □□□ □□□ □□□□ □□□. □□□ □□□□□ SSL □□
□ □□ □□□ □□ □□□ □□□□ □□□ VM□ Cortex XSIAM □□□□□□ □□□□□ □□□
□□ □□□ □□□ □ □□□□?

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

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

SSL □□□ □□ □□ □□□□ □□ □□□□□ □□□ VM□ □ □□ □□ □□□ □□□□□.1.
□□□ □□: □□□ VM □□ □□□□ □□ □□ □ □□□ □□ □□□ □□ □□ □□(IP/□□)
□ □□□ □ □□□□.2. □□□ □□: □□□□ SSL □□□ □□□□□ □□ CA□ XSIAM □□
□□ □□ □□□□□.□□□ VM□ □ □□ □□□□ □□ CA□ □□□□ □□□.□□ □□□□
□□ CA □□□□ □□□ VM□ □□ □□□□ □□□□□ □□□□, □□□□□ □□□ Palo Alto
Networks □□□□□ □□□□□.□□ B□ □□□□ □□□□ □□□□ □□□□.□□ C□ □□
□□ □□□□ □□□ □□□ □□□□□.□□ □□□ □□ □□ □□□□.sh.D□ □□□□ □□
□□.□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□.□□ E□ □ □□ □
□□ □□□ □□□□ □□□□ □□□□ □□□□□.

NEW QUESTION: 82

□□ □□□□ □□ □□□□ □□ □□□□□□ □□ □□□□ □□□ □□□ □□□□ □□□
□. □□□□□□ XSIAM □□□□□ □□□ □□ □□ □□□ □□□□□.

'Registry.Key' □□□ □□□□ □□ □ □□ □□□ □□□□□ □□□□ □ □□ □□□□
XSIAM BIOC □□□ □□□□□? □□□□ □□ □□ □□ □□ □□□ □□ □□□□ □□□□□.

- A.
- B.
- C.
- D.
- E.

Answer: D (LEAVE A REPLY)

The correct answer is D. The question asks for the correct command to run a PowerShell script on a Windows machine. Option A is incorrect because it uses the wrong command syntax. Option B is incorrect because it uses the wrong command syntax. Option C is incorrect because it uses the wrong command syntax. Option D is the correct command to run a PowerShell script on a Windows machine.

NEW QUESTION: 83

A company is using XSIAM for user authentication and AWS CloudTrail for logging. The company wants to create a query to identify users who have successfully authenticated and then run instances on EC2. The company wants to use XQL to query the data.

- A.
- B.
- C.
- {< >}:
 - D.

Answer: D (LEAVE A REPLY)

The correct answer is D. The question asks for the correct XQL query to identify users who have successfully authenticated and then run instances on EC2. Option A is incorrect because it does not filter for successful authentication. Option B is incorrect because it does not filter for EC2 instances. Option C is incorrect because it does not filter for successful authentication. Option D is the correct XQL query to identify users who have successfully authenticated and then run instances on EC2.

D. XSIAM은 '스택 기반 보안'을 제공하는 오픈 소스 보안 플랫폼입니다.

E. XSOAR은 오픈 소스 보안 플랫폼으로, 다양한 보안 솔루션을 통합하여 관리할 수 있습니다.

Answer: A,B,C,D,E (LEAVE A REPLY)

스택 기반 보안, 오픈 소스 보안 플랫폼으로, 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. -A(스택 기반 보안): 스택 기반 보안은 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. -B(스택 기반 보안 플랫폼): XSOAR은 오픈 소스 보안 플랫폼으로, 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. 스택 기반 보안 플랫폼(CPU, 메모리)은 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. -C(스택 기반 보안/SAST/DAST): 스택 기반 보안 플랫폼(SAST, DAST)은 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. -D(스택 기반 보안): XSOAR은 오픈 소스 보안 플랫폼으로, 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. -E(OS/스택 기반 보안): 스택 기반 보안 플랫폼은 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. OS 기반 보안 플랫폼(Python 기반, 오픈 소스)은 다양한 보안 솔루션을 통합하여 관리할 수 있습니다.

NEW QUESTION: 86

기업은 현재 15,000개의 서버를, 500개의 데이터베이스, 20개의 스토리지 서버를 보유하고 있습니다. Palo Alto Networks XSIAM을 도입하여, 현재 10TB의 데이터를, 향후 20TB의 데이터를 저장할 수 있도록 확장할 계획입니다. XSIAM은 현재 90%의 성능을, 향후 10%의 성능을 유지할 수 있도록, 현재 70%의 성능을 유지할 수 있도록 XSIAM을 도입하여, 현재 100GbE의 성능을 유지할 수 있도록 XSIAM을 도입할 계획입니다?

- A. CPU 성능을 향상시킬 수 있습니다.
- B. IOPS 성능을 향상시킬 수 있습니다. NVMe SSD를 사용할 수 있습니다.
- C. GPU 성능을 향상시킬 수 있습니다.
- D. 데이터베이스 성능을 향상시킬 수 있습니다, 스토리지 성능을 향상시킬 수 있습니다.
- E. XSIAM을 도입하여 100GbE 성능을 향상시킬 수 있습니다.

Answer: (SHOW ANSWER)

XSIAM은 오픈 소스 보안 플랫폼으로, 다양한 보안 솔루션을 통합하여 관리할 수 있습니다. NVMe SSD는 IOPS 성능을 향상시킬 수 있습니다. (B) 데이터베이스 성능을 향상시킬 수 있습니다. (E) 스토리지 성능을 향상시킬 수 있습니다. CPU 성능을 향상시킬 수 있습니다, GPU(C) 성능을 향상시킬 수 있습니다. XSIAM은 CPU, GPU, 스토리지 성능을 향상시킬 수 있습니다.

□□□ □□□□□ □□ □□□□□, □ □□□ XSIAM□ □□ □□□ □□ □□□□□ □□□ □ □□ □□□, □□□ □□□□□□ □□ □□□□ □□(D)□ □□□□ □□□□□.

NEW QUESTION: 87

XSIAM □□□□□ C2 □□□□ □□□□□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□ □□□□ □□□□. □□ □□□ □□□ C2 IP □□□ □□ □□□ □□□□□. □□□ □ □□□ C2□ □□□□ □□□ □□□□ □□ □□□□. □□□□ □□ □□□ □□□□□ □□ □□□□□ □□□ □□□□□ □□□. □ □□ □□□ □□□□□ □□□□ □□□ □□ □□ □□□□ □□ XSIAM□□ □□ □□□□ □□□□ □ □□□ □□ □□□ □□□□□?

- A. □□ □□ □□□ □□□□ □□□□□ □□□ C2 IP □□□ □□□□ XQL Sin' □□ □□□□ □ □□□ □□□ □□□□□.
- B. □□ □□□ XQL □□ □□□ C2 IP□ □□□□ □□□ □□ □□□□□ □□□ □□□□ □□ □□ □□ XSIAM□ □□ □□ □□(EDL) □□ Cortex □□□ □□□(CDL)□ □□□□□.
- C. □□□□ IP □□ □□□ C2 □□□ □□□□ □□□□□ □□□ □□ □□□ '□□□□'□□□ '□ □'□□ □□□□□.
- D. XSIAM□ □□□ '□□□□□ □□□□□'□ □□□ □□ □□□ C2 IP□ □□ □□ □□□□ □□ □ □□□□□ □□□□□.
- E. □□□□□□□ XSIAM □□□□□ □□□□ □□□□□ □□ □□□ □□ □□ □□□□□ □ □□ □□□□ □□ C2 □□□ □□□□□ □□□□□.

Answer: B (LEAVE A REPLY)

□□ B□ □□ □□□□□ □□ □□□ □□□□□□. XSIAM□ □□ □□ □□(EDL)□ □□ □□ □□□□□□ □□□□□ □□□ □□ □□□ □□□ □ □□ Cortex Data Lake(CDL) □□□ □□ □□□□□. □□ □□ □□ □□□ □□ □□ □□ □□ □□□□ □□□□□□ IOC □□(□: C2 IP)□ □□□ □ □□□□ □□□ □□□ □□ □□□ □□□ □□□□□. □□ A□ □□□□□ □ □□□□ □□□□. □□ C□ □□ □□□ □□□□ □□ □□ C2 □□□ □□□□ □□ □ □□□ □. □□ D□ □□□□ □□ □□□□ □□ □□□ □□□□□. □□ E□ □□ □□ □□□□ □□ □□ □□□□□□.

NEW QUESTION: 88

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89

□□ XSIAM □□ □□ □ □□□ □□□□ □□ '□□ □□' □□□□□ □□□□□ □□□ □□ □□□□□? (□□□□ □□ □□ □□)

- A. □□□ □□□

- B. 00 00
- C. 00
- D. 00 000 00
- E. 00 00

Answer: B,C,E (LEAVE A REPLY)

0 000 000 000000.A 000 000: 000 0000 00 000 0000 00 00
 00 00000 00 000 00 000 0000000 00 0000 00000.00 000 0
 00 000 00000 000 '00' 000 00 0000 00000 000 000 000 0
 00 000 00 000 00000.B. 00 00: 00 000 00 00 000 00 00 000
 00000.00 000 000 000 000 000 000 00000.000 00 000 00 00
 0 000 00000 0 00 00 000000.C. 00: 00 000 000 '00' 00000 00 0
 000 00000.000 000 000000.D. 00 000 00: 000 000 00 000 0
 000 000000 00000 0 000000.00 00 00000 00 0000000 00 00000
 00000. E. 00 00: 00 000 000 000 000 000 000 00000 00 000
 00000 000 000 00000 00 00 00(0: 000 00 00 00, 00 00, 000 0
 00 00)0 000 00 000000. 00 00, '00 IP0 trusted_ips 000 00 00 000
 00000'0 00 000 0 00000. 000 00 00, 00 0 00 000 00 000 00 0
 00000 000000 000000.

NEW QUESTION: 90

XSIAM 000000 00 CMDB 000 00 00000 'asset_criticality' 000 00 00 000
 0 00000 00000 00 000 000 00000 000. 'High' 00000 000 000 000
 000 000 00 00000 00, 'Low' 00000 000 000 000 000 000.
 'alert.asset_criticality' 000 'High', 'Medium' 00 'Low' 0 00000 000 0, 00 000 00
 0 00 0 00 000 00 00 XQL 00 00 0 0 0000000 00 0 00000 00 000
 00?

- A. 00: 'alert.asset_criticality = '00' 00: 000 +30; 00: 'alert.asset_criticality = '00' 00:
 000 -15. 00 00 000 00 0 00 00 00 00000 000000.
- B. 00: 'alert.asset_criticality in ('High', 'Low') 00: (alert.asset_criticality = 'High') then
 SetTotalScore(90) else SetTotalScore(30)'.
 C. 00: 'alert.asset_criticality = '00" 00: 00 x2.0; 00: 'alert.asset_criticality = '00' 00:
 00 x0.5. 0 00 00 00 00000 000000.
- D. 00: 'alert.asset_criticality = '00" 00: 00 +'alert.base_score 0.5; 00:
 'alert.asset_criticality = '00' 00: 00 '-alert.base_score 0.2.
- E. 000 XQL case 00 00 00 00 0000 000000.

Answer: A,C (LEAVE A REPLY)

00 A0 C0 XSIAM0 00 000 00000 00 00000 00 000000 00000 00000
 0.00 A(000 00 00): 000 000000 000 000000.'00' 000 000 000
 00 000 '00' 000 000 000 0 00 000 00000.000 000 000000 00
 000000.00 C(000 00 00): 00 00 00 00000 000000.2.00 000 '00' 0

0.5 '00' 000 000000 0000 000000. B(00 00 000 '00 00'): '00 00' 000 0 000 XQL00 00 00 00 00 000 'if/then/else' 00 0000 00 00 000 00 XSIAM 00 000 000 00000 00 00 0000. '00 00' 000000 00000 00000, 000 00 000 00 000 0 00 0000 0 00 000 00 000000. 0 00 000 00 000 00 000 0000 000 00 000 '00' 00 '00'0000 0 000000 00 0 00000. 00 D('base_score' 00 00 00): 0000000 000000 XSIAM 00 00 000 00 000 00 000 00/00 0 00 '00 00' 000000. '00 00 00' 00000 'alert.base_score 0.5' 0 0 00 000 00 00000 00 00 00 UI 00 00 000 00000. 00 E('case' 00 00 00 00): XSIAM 00 000 000 000000 000 000 000 000 00000 000000 000000. 000 00 000 '00' 000 00 000 00 000 '0000' 00 00 00000 00(0: 'SetTotalScore' 00 000 'alert.score' 00) UI 00 00/00/00 0 00 00 00 000 00000 00000 00000 00000. 000000 00 000 00 00 00 000 000 000000.

NEW QUESTION: 91

XSIAM 000 00000 0000, 00 00 000000 000(TIP) 0 000 00 000 000000 000000 000. TIP 00 00(IoC) 00 API 00000 0. XSIAM 000 00000 00000 00 0 000 00000 00 000 IOC 000000 0 000 00000 0 00 000 XSIAM 00 00 00 000 000000?

- A. XSIAM 000 000 00 BI 00000 000.
- B. 00 00 000 00 000 XSIAM 000 00 00.
- C. 000 00 000 00000 XSIAM 00 000000 00 000 000000.
- D. API 00 TIP 00 000000 IOC 00000 000 00 XSOAR 000000 000000.
- E. syslog 00000 00 Cortex Data Lake 0 IOC 00 000000.

Answer: C (LEAVE A REPLY)

XSIAM 000 00 TIP API 000 000000 00 0 00 000 00 00 000000 00 00 (C) 000, XSOAR 00000(D) 00 00000 000 0000000. XSOAR 000000 0 0 00, 00 00, 000 00 000 00, 000 IOC 000 XSIAM 00 000000 000 0 00000 000 0 000 000000. BI 00000(A) 000 00000 00 000, 000 000 00(B) 000 00 00 00000 00 000, syslog(E) 000 API 000 00000 00 0000000 00 000 00 00000. XSIAM 000 00 000000 00 00(C) 000, XSOAR 000000 00 API 000 00000 00000 00 000 0 00 000 000000.

XSIAM-Engineer 00 000 000000 00 DumpTop 00 00000 000 XSIAM-Engineer 00! DumpTop 0 00 **XSIAM-Engineer** 00 000 0000000, DumpTop XSIAM-Engineer 00 000 0000000000 000 000000000. 00000 000 00 00 00 DumpTop XSIAM-Engineer 000 000000. <https://www.dumptop.com/Palo-Alto->

NEW QUESTION: 92

Which XSIAM tool can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues (e.g., OneDrive, Google Drive), Microsoft 365 Exchange Online, and other Microsoft 365 services? XSIAM can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues.

- A. 1. Microsoft 365 (M365), 2. Microsoft 365 (M365) URL, 3. HR (Human Resources) (HR).
- B. 1. Microsoft 365 (M365) (M365), 2. Microsoft 365 (M365) (CASB) (Cloud Access Security Broker), 3. Microsoft 365 (M365) (M365 Audit) (Microsoft 365 Audit).
- C. 1. VPN (Virtual Private Network) (VPN), 2. Active Directory (AD) (Active Directory), 3. Microsoft 365 (M365) (M365 Audit) (Microsoft 365 Audit).
- D. 1. Microsoft 365 (M365) (NetFlow/IPFIX), 2. Microsoft 365 (M365) (IDS) (Intrusion Detection System), 3. Microsoft 365 (M365) (IP) (IP Address).
- E. 1. Microsoft 365 (M365) (M365), 2. HVAC (Heating, Ventilation, and Air Conditioning) (HVAC), 3. Microsoft 365 (M365) (M365 Audit) (Microsoft 365 Audit).

Answer: B (LEAVE A REPLY)

Microsoft 365 (M365) can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues (e.g., OneDrive, Google Drive), Microsoft 365 Exchange Online, and other Microsoft 365 services. CASB (Cloud Access Security Broker) can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues. Microsoft 365 (M365 Audit) can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues. Microsoft 365 (M365) (M365 Audit) (Microsoft 365 Audit) can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues.

NEW QUESTION: 93

XSIAM can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues. 'IP (Internet Protocol) and DNS (Domain Name System) are used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues. XQL (XSIAM Query Language) can be used to identify and remediate security issues, such as misconfigurations, vulnerabilities, and compliance issues.

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

E.

Answer: (SHOW ANSWER)

DD D0 0000 000 00 0000 XQL 000000. 00000 0000 00 00 00000 0 00000. '00' 0000 00(000000 00 0000 0000 00 000000)00 0 0 00 0 00 000000. 0000 0000 'endsWith' 00 'contains'0 00000 00 00000 00 0000 0000 00000, 00 00000 000000 00 0 0 00000. 00 A0 00 0000 00 00 XDR 00000 000000. 00 B0 000000 000000, 'contains'0 'endsWith'00 0000 0000 0 000000. 00 C0 00000 00 00 0000 0000 00 00 0000 000000 00000 0000 00 00000 00 0000 000000. 00 E0 00000 0000 00 XQL 0 00 0000 00 000000.

NEW QUESTION: 94

0000 XSIAM 0000 VM0 0000 0000 0000 0000 0000000 0000 00 0000 0000 0 0000 0000 0000000000. 0000 VM 0000 00000 0 VM0 XSIAM 0000000 00 0 0 00 00 XSIAM 0000 '0000 VM 00000'0000 000000 0000000. 00000 00 0000 00 00000 000000. 0000 VM 0000 00 00 00 0000 0 00 00000 0 00 TLS 0000000 0000 0000000000. 00 0 00 0000 00 0000 00000, 0000 VM0 00 00 0000 00000 0000 0000 0000 0000000?

- A. 0000 VM0 00 00(NTP)0 0000000 00 00 0000 00 0000 0000 0000 00 0000. 0000 VM00 NTP0 00 00000000.
- B. 0000 VM 0000 0000000 00 0000 00 00000 00000 0 0000 0000 00 0 00 0 00 CA 00000 0000000000 0000000000. 00000 00 CA 00000 0000 VM0 00 00000 00 00000 0000.
- C. 00000 00 0000 VM0 0000 0000 00 00 0000 0000000000. 0000 0000 0000 0000000 00 0000000.
- D. 0000 VM0 00000 0000000 0000 0000000 00 000000000 0000000000. 0 0000 0000 00 0000000.
- E. XSIAM 00000 0 000000 000000 00 0000 VMS0 0000 000000. Palo Alto Networks0 0000 0000000.

Answer: B (LEAVE A REPLY)

00 0000 '0000 0 00 00000 0000 TLS 0000000 00'0 '0000 0000 0000 00 0 0000000 0000 00 0000 00 0000 00'0000. 0000 00000 00000 SSL/TLS 0000 0 0000000 000000 00 000000 0000 VM0 000000 0000 000000. 0000 VM0 0 0000 00 000000 00000000 000000 00 CA 000000 0000 VM0 0000 0 00 0000 000000 000000 0000. 0000 0000000 0000 0000 00 0000 000000 00 0000 00 0 000000. 00 A, C, D0 00 00 000000 00000000 000000 000000. 00 E0 000000 0 0000 0000 0000 VM00 0000 00 0000 VM0 0000 000000.

NEW QUESTION: 95

XSIAM can be configured to generate alerts for various types of events. Which of the following is not a valid alert type?

- A. IP addresses associated with a specific user name.
- B. 'network_connection' events with 'application_name' set to 'web-browsing' and 'ftp'.
- C. Events with 'remote_ip_address' in the list of 'sanctioned_ips' or 'url_hostname' in the list of 'sanctioned_urls'.
- D. XSIAM events with 'user_name' set to 'not in' and 'application_name' set to 'not in'.
- E. XSIAM events with 'user_name' set to 'not in' and 'application_name' set to 'not in'.

Answer: (SHOW ANSWER)

The correct answer is B. XSIAM can generate alerts for events where the 'application_name' is 'web-browsing' and the 'remote_ip_address' is in the list of 'sanctioned_ips' or the 'url_hostname' is in the list of 'sanctioned_urls'. However, XSIAM does not generate alerts for events where the 'application_name' is 'ftp'.

NEW QUESTION: 96

XSIAM can be configured to generate alerts for various types of events. Which of the following is not a valid alert type?

Which of the following is a valid IP address for a host in the 10.10.10.0/24 network?

- A. 10.10.10.1
- B. 10.10.10.255
- C. 10.10.10.10
- D. 10.10.10.0
- E. 10.10.10.254

Answer: C (LEAVE A REPLY)

Which of the following is a valid IP address for a host in the 10.10.10.0/24 network? The correct answer is 10.10.10.10. The other options are either the network address (10.10.10.0), the broadcast address (10.10.10.255), or addresses that are not in the 10.10.10.0/24 range (10.10.10.1 and 10.10.10.254).

NEW QUESTION: 98

Which of the following is a valid IP address for a host in the 10.10.10.0/24 network? The correct answer is 10.10.10.10. The other options are either the network address (10.10.10.0), the broadcast address (10.10.10.255), or addresses that are not in the 10.10.10.0/24 range (10.10.10.1 and 10.10.10.254).

- A. 10.10.10.1
- B. 10.10.10.255
- C. 10.10.10.10
- D. 10.10.10.0
- E. 10.10.10.254

Answer: C (LEAVE A REPLY)

Which of the following is a valid IP address for a host in the 10.10.10.0/24 network? The correct answer is 10.10.10.10. The other options are either the network address (10.10.10.0), the broadcast address (10.10.10.255), or addresses that are not in the 10.10.10.0/24 range (10.10.10.1 and 10.10.10.254).

XXXXXXXX. XX BX XX XXXXXX XXXXX X XXX, XXX XX XXXXX XXXXX XX
XX XX XXXXX XXXXX XX X XXXXX. XX AX EX XSIAMX XXXX XXXXX XXXX
XXX, XX DX XXXX XXXXX XXXXXXX.

NEW QUESTION: 99

XSOAR XXXXXX XSIAM API XX "Cxsiam-api-v2-get-alert-raw-data")X XXXXX XXXX XX
X XX XXXX XX XXXXX XXXXXXX. X XXXX XX IDX XXXXX XSIAMX XXXX XXXX
XXX 'KeyError: 'raw_data'X XXXXX XXXX XXXXX. XX XX XX XXXXX XXXX XX
API XXXXX 'raw_data' XXXX XXXXX XXXX XXXX XXXXXXX. XXXX XXXXX XXXXX
XXX XXXXX XXXX XXXX X XX XXXX XX XX XXXXX XXXXX XXXX XXXXXXX
X X XXXX XXXX XXXXX XXXX?

- A. 'xsiam-api-v2-get-alert-raw-data'X XXXXX XX 'wait' XXXX XXXXX XX XXXXX XSIAM
X XXXX XXXXXXXXX XXXXXXX.
- B. 'raw_data' XX XXXXX X XXXXX XXXXX Python '.get()' XXXXX XXXXX(X:
'response.get('raw_data', OF)) XXXXX XXXXX XX XXXX XXXXXXX.
- C. API XX XX XX XXXX 'try-except KeyError' XXXX XXXXX 'KeyError'X XXXXX XX
XX XXXXXXXX XXXXXXX.
- D. XXXXXXX XXXXXXX XX XX XX XXXX XX 'raw_data'X XX XXXXXXX XSIAM 'XX
XX' XXXXX XXXXXXX.
- E. XXXXXXX 'xsiam-api-v2-get-alert-raw-data' XXXX *is-error'X XXXXX XX(X: 'KeyError')X
XXXXX XXXXX XXXX XX XXXXXXX XXXXX 'XXXX' XXXX XXXXX.

Answer: B,C (LEAVE A REPLY)

'KeyError'X XX XXXXX XXXX XXXXXXX. XXXX(B)X XXXXX .get()'X XXXXX XX
'KeyError'X XXXXX XX Python XXXXX, XX XXXX XXXXX XXXXXXX XX XXXX X X
XX XXXX. XXXX XXXXX XXXX XX XXXX XXXXX X XXXX XXXX. XXXXX 'try-
except KeyError' XX(C)X XXXXXXX XXXX XXXXX XXXXX XXXXXXX. XX XXXX X
XXX XX XX XXXX XX XX XXXX XXXX XXXXX X XXXX XX XXXXXXX. BX CX
XX XXXXX XXXX XXXXX XXXXXXX. XX AX XXXX XX XX XXXXX XXXXX X X
X XXXX XXXXX XXXX XXXXX XXXXX. XX DX XSIAMX XX XXXX XXXX XXXXX
XXX, XX XX XXXXX XXXX XXXXXXX XX X XXXXX. XX EX XXXX XXXX XX X
XX XXXXXXX, XX BX CX XX XX XXXX X XXXXX XXXX XXXXXXX.

NEW QUESTION: 100

XSIAMXX 'XX XXXXX XX XX' XXXXXXX XXXXX XXXXX. XXXX XX XXXX XXXX
XXX XXXXX XX XX XXXX XXXXX XXXXXXXXXX XXXX XX XXXX XXXXXXX XX
XX. XX XX XXXXXXXXX XX(X: process_events, network_connections)X
'data_store_access_logs'X XXXXXXX, XXXXXXXXXX XX XXXX XX XX 'XX' XXXX X
XXXXX XXXX. XX, XXXXXXXXX XXXX XXXX XXXXX XX 3X XXXXXXXXXX XX 24
XX XX XXXX XX XXXX XXXXXXX XXXX. XXXX XXXX XXXXXXX XXXX XXXXX X
XX XXXX XSIAM XQL XXXX XXXX XXXX XXXXXXX?

