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

NEW QUESTION: 2
□□ □□ □□(SOC)□□ Palo Alto Networks XSIAM□ □□□□ □□□, □□ □□ □□(□: AbuseIPDB, VirusTotal)□ □□ □□□□□□ □□□□ □□□□ □□□ IP □□□ □□□□ □□ □□□ □□□. □□ □□□□□□□ □□ □□□□□ □□□ □□□ □□ □□ □□□ □□□□ □. □□ □ □□ □□ □□□□□ □□□ □□□□ □□□ □□□ □□ □□□ □□□ □□□□ □ □ □□□□□ □□ □□□ □□□ □□□□□?
A. □□□ □□□ □□ □□□□□ □□□ □□ □□ □□□□□ □□□□ □□□□ XSIAM □□ □□ □□ □□□ XSOAR □□□ □□ □□ □□□□□□.
B. □□□ □□ □□□□□ □□□□ □□□ XSOAR □□□ □□□□, □□ □□□ □□□ □□□ □□ □□ □□□ □□ XSIAM □□□□□□□ □□□□□.
C. □□ □□□□□□ □□□ □□ □□ YAML □□□ □□□□ □□□ □□□ □□ API □□ □□ □□□ □□□ □□□□ □□, □□□□□ □□ □□ □□□□□.
D. XSIAM□ □□□ '□□□ □□□'□ □□□□ □□□ □□□□ □□ □□ □□□□□□ □□□ □□ XSIAM □□□□□ □□□□ □□□ □□□□ □□□□□.
E. □□ □□□□□□ □□□ □□ □□□ □□□□□ □□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□ □□□□□ □□□□ □□□□ '□□ □□ □□□□□□□' □□□ □□ □□ □ □□□ □□ □□□ □□□□.
Answer: E (LEAVE A REPLY)
□□ E□ □□ □□□□□ □□□□ □□□□□. □□ □□ □□□□□□□ □□□ □ □ □□ □ □□ □□□ □□□□□ □□ □□□ □□□□ □□ □□ □□□□□ □□□ □□ □□ □□□ □ □ □ □□□□ □ □□□□. □ □□□ □□□□ □ □□□ □□ □□□ □□□□□□ □□□ □□□ □□ □□ □□ □□ □□□ □□ □□□□□ □□□□□□ □□□ □□ □□□□□ □□□ □ □ □□□. □□ □□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□ □ □□□□. □□ A□ C□ □□□□ □□ □□□□ □□□□□. □□ B□ □□□ □□ □□□□□ □□ □□ □□□□ □□ □ □□□□ □□□□□. □□ D□ □□ □□□□□□ □□□ □ □□ □□□ □□□ □□□ □□ □□, □□□ □□□□ □□ □□□□.

NEW QUESTION: 3
□□ □□□□ □□ Linux □□□ Cortex XSIAM □□□□□ □□□□ □□□. □□□ □□□ □□ □□ □□□□ □□□ □ □□□, □□□□ □□ □□□□□ □□□□□ □□ HTTP □□□□ □□ □ □ □□□□. □□□□ □□□□□ □□ □□□ □□□□ □□□□ 'Critical_Servers' □□□□ □□□ □□ □□□□□ □□□ □□□. □□ □□□ □□ □□□ □□□□□?
A.
B.
C.
{<□>}:
D.
Answer: D (LEAVE A REPLY)
□□ E□ □□ □□□□ □□□□□. Linux□ Cortex XSIAM □□□□ □□ □□□□□ □□□□ □ □□□ □□□ □□□□ □□ '-proxy-string'(□□□ □□ □□ □□□)□ □□□□□ □□ □□

□ □□□□ □□ '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 □□□ □□ '□□ □□□ □□ □□□ □□□□ □□' □□□ □□□□ □□□□ □□□□. □□□ □□□□ □□□ □□□□ □□□ □□□□ □□□ □□ □□□□□□ □□□□ □□ □□□ □□□□ □ □□□ □□□. □□ □□□□□□, □□ □□□ □□ □□□ □□□□□ □□□ □□□□ □□□ □□ ASM □□ □□□ □□□ □□□□□□□□□?
A. □□□ □□□□□ '□□□□□ □□ □□□ □□□□ □□' ASM □□□ □□□ □□□□□□ □.
B. □□ ASM □□ □□ □□ □□ S3 □□ □□□□ □□□ □□ □□ □□□ □□□□.
C. '□□□□□ □□ □□□ □□□□ □□' □□□ XQL □□□ □□□□ □□ 'public_content_delivery' □□□ □□ □□□ □□□□ □□□ □□□□.
D. □ □□ S3 □□□ □□ □□ □□□□ '□□' □□ '□□'□ □□□□□.
E. □□ □□ □ □□□ □□ S3 □□□ □□ □□□ □□□□ □□□□ SOAR □□□□□ □□□ □□.

Answer: (SHOW ANSWER)

B□ C□ □□ ASM □□ □□□ □□□□□ □□□□ □□□ □ □□□□ □□□□ □□□□□.
□□ B(□□ □□ □□)□ XSIAM□ □□□ □□ □□□ □□ □□ □□□□ □□□□□ □□□ □ □□□□. □□ C(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: □□□ □□/□□□ □□□ □□ □□□: □□ □□ □□□□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□□. □□□ □□□ □□ □ □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□□ □□ □□□□ □□□□□. □ □□□ □□□ □□ □□□ □□□ □□□□ XSIAM□ □□□ □ □□ □□□/□□ □□□ □□□ □ □□ □□□□ □□□ □□□□. □□ B(risk_score □□□)□ □□ □□□ □□ □□□ □□□

□ □□ □□ □□□ □□ □□ □□□□□. □□ □□□ □□□□□ □□□ □□□□□□□□ □ □ □ □□□□. □□ E(□ □□ □□ □)□ □□□□□ □□□□ □□□ □□ □□□□ □□□□□ □□□□ □□□, □□□ □□□ □□□ □□□ □□□ □ □□□□.

NEW QUESTION: 7
□□□ XSIAM □□□□□ □□□ □□ □□□□□□ □□□ □□□ □□□□ □□□□□. □□□ □□ □□□□□ □□ □□□ □□□□ □□□□ □□□, □□□□□□ □□□ □□□□ □□ □ □□ □□□□ □□□ □□□□ □□□□□. □□ □□ □□ XSIAM□ □□ □□□ □□□ □□, □□□ □□ □□□□ □□□□ □□ □□ □□('transaction_value')□ □□□ □□ 'N/A'□ □□□ □ □□ □□□□□□. □ 'N/A'□ □□ □□□□□ □□□ □□□□□ □□□ □□□ □□□□□. XSIAM□ □□ □□□□□□□ □ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□□□□□ 'transaction_value'□ 'N/A'□ □□□□ □□□□□ □ □□□□ XSIAM □□□ □ □□□□. □□□ □□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□□ □□□□ □□□ □.
B. XSIAM □□ □□ □□ □□ □□ □□ □ □□□ □□□□ 'N/A'□ 'null'□ □□□□□ 'transaction_value' □□□ □□ □□□□□ □□□□□ 'mutate' □□ 'replace' □□□ □□□□□. □ □□□ □□□ □□ □□□□ □□□.
C. □□□□□□ □□□□ □□□□ □□ □□□ 'N/A'□ □□□□ □□□ □□□. □□ □□□□ □□□ □□□□□□ □□ □□ □□□□ □□□□ □□□□□ □□□□.
D. XSIAM□□ 'transaction_value' □□□ □□□□ 'number'□□ 'string'□□ □□□□□. □□□ □□ 'N/A'□ □□□□□ □□ □□□ □□□□□□.
E. XSIAM Data Lake □□□ □□□□ □□□ □□□ □□□□□ □□□ □□ □□□ □□□□□ □□□ □ □□□□. □□ □□□ □□□ □□□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
□ □□□□□ □□□ □□ □□ □□ □□□ □□□□ □□□ □□□□ □□□ □□ □□□ □□ □□□. □□ □□□□□□□ □ □□□ □□□□ □□ □□□ □□□ □□ □□ □□ □□□ □□ □□ □□□□ '□□'□□ □□□□. □□ B□ □□□ □□ □□□□□. XSIAM□ □□ □□ □□ (□: 'mutate' □□ 'replace' □□)□ □□□□ 'N/A'□ □□ □□ □□(□: 'null' □□ 'os')□ □□□□ □□□ □□□ □ □□□□ □□□□□ □□□□. □□ A□ □□□ □□ □□□, □□ C□ □□□ □ □□□□□ □□□□ □□□□ □□□□. □□ D□ □□□ □□□□ □□□□□. □□ E□ □ □□ □□□ □□□□.

NEW QUESTION: 8
XSIAM □□□□ □□ □□ □□□□ □□□ □□□□ □□□ □□□□□□□ □□□, □ □□□ □□ □□ □□(□: □□□□□ 1~19, □□□ □□ 20~35, event_id 36~40)□ □□□□□. □□ □ □□ □□□ □□ □□□□□□. □□□ □□ □ □□□ □□□□□ □□ □□□ □□ □□□ □□ □□□ □□□ □□ □□□ □□□□, □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□ □□□ □ □□□□?
A. □□ A
B. □□ B

C. □□ C
D. □□ D
E. □□ E
Answer: (SHOW ANSWER)

NEW QUESTION: 9
'□□□□ □□' □□□ □□□□ XSIAM □□□ □□□ □□□. □□□ □□□□ 'source_ip', 'destination_ip', 'source_port', 'destination_port', 'protocol', 'application_name'□ □□□□ □□□ □□□□. □□□ □□□ □□ 'application_name'□ □□□□ □□ □□(□: 'http', 'HTTP', 'WebTraffic', 'Port 80'), 'source_ip'□ □□ □□□□□ □□□□ □□□ □□ □□ □□ □□□□□ □□□ □□□□□□ □□□□□ □□□ □□□□□□. □□ □□ □ □□□□ □□□ □□□□□ □□ □□ □□□□□ □□ □ □□□ □□□□□□ □□□ □□ □□□□ □□□□□□, □□□ □□□ □ □□□ □□ □□□ XSIAM □□□ □□□ □□ □□□ □□□□□?
A.
B.
C.
{<□>}:
D.
Answer: (SHOW ANSWER)
□ □□□ □□□ □□ □□ □□ □□ □□□□ □□ □□□□□□ □□□ □□□□□ IP□ □□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□.A□ E□ □□ □□□ □□ □□□ □□□□ □ □□□□□.□□ A: - □□ 1(map_field): □□ □ □□□□ □□ 'application_name' □□ □□□ 'normalized_application'□ □□ □□□□ □□ □□ □□□ □□□□□.□□ □□□ □□□□ □ □ □□□□□□.- □□ 2(□□□ □□ □□ □□): 'source_ip'□ □□□ □□ □□□□ □□□ □□ □ 'destination_ip'□ □□□□□.□□ □□ IP □□□□□ □□ □□□ □□□□ □□ IP□ □□□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□ □□□□□ □□□ □□□□□□.□□ E: - □ □ 1(map_values□ □□□ □□): □□ A□ □□□□, □ □□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□ □ 'application_name'□ □□□□□ □□□ □□□□ □□□□□. - □□ 2(□□□ □□□ □□ enrich_field): □ □□□ 'destination_ip'□ □□□ IP □□□ □□□□□, □ □□ □□ 'source_ip'□ □□ IP□ □□□ 'application_name'□ 'Internal_' □□□□□□□ □□ □ □□□ □ □□□ □□□□□ □□□□. □□□ □□ □□□□□ □□□ □□ □□□□□□□ □ □ □□□□ □□ □□ □□ □□ □□□□□□ □□ □□□□□□ □□□□ □□ □□□□. □□ □□□□ □□ □□□ □□□ □□□□□□□□. □□ □□□□ □□□□□ □□ □□□ □□□ □□□□. - □□ B□ □□□ □□ □□□□ □□□ □ 'join_with_dataset'□ □□□□□. □□□□ □ □□□□□□□, □□ □□ □□ □□□ □□□□ □□(□□ □□/□□□□□ □□ □□) □□ □ □□□ □□ □□ □□ □□□□ □□□ □□□ □ □□□, □ □□□ □□ □□ □ □□□□ □ □□ □□□ □□ □□□□□. □□ □□□ IP □□□□□□ □□□□□ □□□□ □□□□. - □□ C□ □□□ □□ □□□□ □□□□□, □□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □ □□ □ □□□□. IP □□ □□□ □□□□□ □□□ □□□□□□ □□ □□□□□ □□□□. - □□ D□ □□□□□□□ □□ □□ □□ □ □□□ □□□□ □□□ □□□□□, □□□ □□□

□□ □ □□□□□□. 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 □)□ □□□□ □□□ JIT □□ □□□ □ □□□□. PAM □□□□ □□ □ □□ □□□□□ □□ □□ □□ □□ □□□ □□□□ □□□ □, XSIAM□ □□□ □□ □□ □□□□ □□□ □□□ □ □□□□. □□ □□ □□□□ □□□ □□□□□. □□ D□ XSIAM □□□ □□ □□□□□ □□□□□□□ □□ □□□□□. XSIAM □ □□□ □□□ API□ □□□□ □□□ □□□ □□□□ □□□□□ □□□ □ □□□□. □□ □□□□ □□□ □□□ □□□ □□□□□ □□ □□□□□. □□ B□ □□ □□□□ □□ □□ □ □□□□ □□, □□□ JIT □ □□ □□ □□□ □□□□□. □□ C□ □□□□ JIT □□ □□□

□□ □□□ '□□ □□'□ □□□ □□□ □□ □□□□. □□ E□ IdP □□□ □□□□□, □□ □ □□ □□, □□ □□□, □□□□□□□ □□ □□ □□□ □□□□□ □□□□ □□ □ □□□□.

NEW QUESTION: 12
□□□ XSIAM□ □□ □□ □ □□□□ □□ □□ □□□ □□□□ □□□□. □□ □□□□□□ PKI□ □□□□ □□ □□ □□□□ □□ □□□ □□□ □□□□ □□□□. □□□ □□ □□□ □□□ □□□□ □□□□□ XSIAM □□□ □□□□ □□, XSIAM □□□ □□□ □ □□ □□ □ □□□ □□□ □□□ □□ □□ □ □□ □□□ □□ □□ □□□ □□□□, □□ □□ □□□ □ □□□ □□ □□□□ □□□?
A. □□□ □□□□ XSIAM □□□ □□□ □□□ □□ □□ CA□□ □□□ □□□□□ □□□□ □□□□□. □□ □□ □□□ □□□□□ □□ □□□ □□□□□.
B. □□□ □□□□ XSIAM □□□ □□□□ □□ □□(□□ TLS□ □□□ □□)□ TLS□ □□ □ □□□ □□ □□ □□(□: □□ Syslog)□ □□□□ □□□□ □□ □□ □□□□□□ CA□□ □ □□ X.509 □□□□ □□□□□. □□ □□□ □□□□ XSIAM □□□ □□□□ □□ CA □□□ □ □□□□ □□□.
C. □□ □□□ Palo Alto Networks□ □□ □□□ □□□□□ □□ □□□□□ □□□□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□□.
D. XSIAM □□□ □□□□□ □□□ □□□□ □□□□□. □□□ □□□□□ □□ □□□ □□ □□□□ □□□□ □□□□.
E. □□□ □□□□ □□□ □ □□□ □□ □□ □□□ □□□□ □□ 24□□□□ □□□ □□ □ □ □□□□ □□□□ □□□.
Answer: B (LEAVE A REPLY)
□□ B□ □□□ □□ □□□ □□□□. □□□ □□□□ □□□ □□□ □ □□□ □□, □□ TLS □ □□□ □□□□ □□□□□ □□□□ □□□□□ □□□□ □□□ □□□, □□ □□□□ □ □ □ □□□□ □□□□□□ CA□□ □□□□ □□ □□□□□□. □ □□□ □□ □□ □□ □ □□ □□□□ □□(□: □□ Syslog)□ □□□ □□□□ □□□ □□, □□□ □□□□ □□ □□ □ □□ □□□ □□ □□□ □□□□ □□□(□□□□□□ CA□□ □□)□ □□□□ □□□ □□ □□. □□□ □□□□ □□ XSIAM □□□ □□□□ □□ □□□(□□□□□ □□ CA□□ □□) □ □□□□ □□□. □□ A□ □□ □□ □□□ □□□□□. □□ C□ □□ TLS/PKI□ □□□□ □ □□□□ □□□□. □□ D□ □□□ □□□ □□□ □□□□ □□□□. □□ E□ □□□□□ □□ □□□□ □□□□(□□ □□). □ □□□ □□□ □□□□ □□□□(□□ □□□□) □ □□ □□□(□□□ □□□□) □□□ □□ □□□□.

NEW QUESTION: 13
□ □□□□□ XSIAM□ □□□□ □□□, □□□ □□□ □□ □□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□. □ □□□ □□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□ □ □□□□. □□ XSIAM □□□ □□ □□ □□□ □□ □□□□□ □□ □□□□ □□□□□□. □□ □ XSIAM □□□ □□□ □□ □ □□ □□ □□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□□ □□ □□□ □□□□ □ □□ □□□□ □□ □□□□□?

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

Answer: (SHOW ANSWER)

□□ B□ □□ □□□□ □□□□□. □□□□, □□, □□□ □□□ □ □□ □□ □□□ □□□ □□□□ □□□ □□□ □□□□□□ □□□□ □□□ □□□□ □□□□□ □□□□□. □□□ □ □□□□ □□□ □□□ □□□□□□ □□□ □□□ □□□ □□□ □ □□□□. □□ A□ E□ □□ □□□□ □□□ □□□□ □ □□ □□□ □□□ □□□□ □□□□. □□ C□ □□□ □□ □□□ □□□□□ □□□□□. □□ D□ IJEBA□ □□□□□, □□□□□ □□ □□ □□ □□□ □□ □□□ □□□□ □□□ □□□□ □□ □□ □□□□□□.

NEW QUESTION: 14

□□□□ □□□□ □□□ XSIAM □□□ □□□□ □□□□ □□ □□□□ □□□ □□ □□□□ Amazon Kinesis Data Stream□ □□□□ □□ □□□□□□. XSIAM□ □□□ □□□□ □□ □ □□□□ □□□□ □□□□ □□ □□□ □□□ □ □□□ □□□ □□ □□□□□ □□□□ □ □ □□□ □□□□□?

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

Answer: B (LEAVE A REPLY)

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

□□□ □□□□. □□ 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

HTTPS POST□ □□ □□□□ □□□ □□ □□□ □□ □□□ □□ XSIAM □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□ Python □□□□ □□□ □□□. □□□ JSON □□□□□□ '□□□ ID'□ '□□□ □□'□ □□ □□ □□ □□□ □□□□ □□□□. □□□ □□□ □□□□ □□ □□□ □, □ □□ □□□ □□ □□□ □□□□ □□ □□ XSIAM API □□ □□ □□□□□ □□ □ □□□□□□ □□ □□□ □□ □□□□□?

A.

B.

C.

D. □□□ □□□□□ □□□□ XSIAM '□□□ □□' □□□ □□□□. □ □□□ □□□ UI □□ □□□□□□ □□□ JSON □□ □□□ □□ API□ □□ □□□ □□□□ □ □□□□.

E. XSIAM □□□ □□ API□ □□ □□(x-api-key)□ □ □□ □□□□ □□□□. OAuth 2.0 □□ □□□ □□ □□ □□□□□.

Answer: B (LEAVE A REPLY)

□□ B□ □□□ □□ □□ □□ 'parser' □□□□ □□□ □□ □□□ □□□□ □□□□□. □□ □□□□(□□ JSON)□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □ □, XSIAM API□□ 'parser' □□□ □□□□□. □ 'parser'□□ □□□□□ parser□ 'type'(□: 'json', 'regex')□ □□ □□□ □□□□ 'mapping' □□ 'rules'□ □□□□□. □□□ □□□ □□ □ □□ 'fields' □□□ □□ □□□ □□□□ □ □□□□, □□ □□□ □□□□ □□□□. □□ A□ □□□□ API □□□□□ □□ □□□ □□□□ □□□□□, □□ □□□ □□□□ □□□□□. □ □ C□ 'type' □ □□ □□□ □□□□□□□. □□ D□ □□□□□□□. UI □□□ □□□, □□□ □□ □□□ □□ API □□ □□□ □□□□□. □□ E□ □□□□□ □□□□□□□. OAuth □ □□□ □□□ □□□□□□, API □□ □□□□ □ □□□ □□ □□□ XSIAM API□ □□□ □□ □□□□□.

NEW QUESTION: 17

□ □□□ □□□ XSIAM□ □□□□ □□□, □ □□□(BUS)□□ □□ □□ □□ □□□ □□□ □ □□□□. □□□ XSIAM □□ □□□ 'Malware_Execution_Attempt'□ □□ □□□□ □□□□ □□. □□□ BU 'FinTech'□ □□□□ □□□□ □□ □ □□□ □□ □□□□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□ □□□□□□□ □□□□□. SOC □□ □□□ □□ □□ □□□ □□□□□ □□□. 1) BU 'FinTech'□□ □□□□, 2) □□□□ □□□□, 3) □□□ □□□ □□□ □□□ □□□□□□ □□□□□□ □□□ □□□□ □□ 'process.hash' □□ □□

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

A. □□□ □□ □□□□ □□□□□. 1. □□ FinTech □□□ □□ □□□ □□ '□□ □□'□ □□ □□. 2. FinTech □□□□□□□ □□ □□□□ □□□ □□□□ XSIAM '□□ □□ □□(EDL)'□ □□□□ □□□□□□ □□ □□□□□ □□ □□□□□. 3. 'asset.tags CONTAINS 'FinTech' AND 'process.hash IN EDL('FinTech_Benign_Hashes')'□ □□□□ 'AND □□'□ □□□□ □□ □ □□ '□□'□ □□□□.

B. □□□ □□ □□□□ □□□□□. 1. 'source_bu = 'FinTech' □ 'process.hash IN ('hashl', 'hash2', ...y'□ □□ 'NOT' □□ □□□□□ □□□ KQL □□□ □□□□□.

C. □□□ □□ □□□□ □□□□□. 1. □□□ □□□ □□□ FinTech □□□□ □□□□□ □□ □□ Cortex XSOAR □□□□□ □□□□□. 2. □□□□ □□□□□ □□□ □□ FinTech □□□ □□ □□□□□□□ □□□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□.

D. □□□ □□ □□□□ □□□□□. 1. 'alert_name = AND 'source_ip IN'□ □□□□ □□□ XSIAM '□□ □□'□ □□□□. 2. □ □□□ □□□ '□□ □□'□□□. 3. □□□ □□□ □□ □□ □ □□ □□ □□□□□ □□□□□.

E. □□□ □□ □□□□ □□□□□. 1. FinTech □□ □□□ □□ □□ □□□ □□□□ '□□'□ □□□□.

Answer: (SHOW ANSWER)

□□ A□ □□ □□□□□ □□□□ □□□ □□□□□□.□□□ □□ □ □□ □□ XSIAM □□ □ □□□□□.1. □□ □□: BIJ□ □□□□ □□□ □□□□□ □□□□□ □□□□ □ IP □□□ □□□□ □□ FinTech□ □□□ □□□ □□□□□.2. □□ □□ □□(EDL): □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.□□ □□□□□ □ □□□ □□□□□ □□□□□ □□ □□ □□ □□□ □□ □□□ □□□□□ □□□.3. □□ □□: 'AND' □□□□ □□□ □□□ □ □ □□□□ □□□ FinTech□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □□□ □ □□□□□.□□□ □□ □□□□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□□ □□□ □□.□□ B□ □□ □□ □□□□ □ □□ □□□□ □□ □□ □□□ □□□□□.□□ C□ □□ □□□□□ □□ □□□ □□ XSOAR □□□□ □□□□□.□□ D□ □□□□ □□□ □□□□ □ □□ □□ □□□□□ □□□□ □□□ □□ □□□□□□. □□ E□ □□□□ □□□ □, □□ □□□ □□□□ □□□□ □□ □□□ □□ □□□□□ □□□□.

NEW QUESTION: 18

□□ □□□□ □□□ □□ □□□ XML □□□□ □□□□ □□□□□ □□□ □□ □□□□ XSIAM□ □□□ □□□□ □□□□. XSIAM □□ □□□ □□□ □□□□ □□□ □, 'CVSS □□' □ '□□□ □□ □□ IP' □□□ □□□□ □□ □□□ □□□ □□□ □□□□□ □□□. □ □□ □□□□ □□□ XSIAM □□ □□ □□□ □□ □□ □□□ □□□□□?

A. XSIAM □□□ □□□□ □□□□ XML □□□ □□ □□□□ □□□ □□ XSLT □□□ □□ □□ XSIAM □□□ □□□□ □□ □□□ □□□□□.

B. □□□ □□□□□ XML □□□□ □□□□ XSIAM□□ □□□□□ syslog □□□ □□□□□.

C. XML□ JSON□□ □□□□ Python □□□□□ □□□ □□, HTTP □□□ □□□□ □□ JSON □□□□ XSIAM□ □□□□□.

D. XML □□□ □□ □□□□□ □□□ XSIAM□ □□ □□□□□□.
E. XML □□□ □□□□ □□□□ CVSS □□□ □□ XSIAM □□ □□□□ □□□□.
Answer: (SHOW ANSWER)
□□ A□ □□ □□□□ □□□□ □□ □□□□□. XSIAM □□□ □□□□ XML□ □□□ □□ □ □□ □□□ □□□ □ □□□□. □□□ XSIAM □□ □□□ □□ □□(XML □□□ □□ XSLT □□ □□)□ □□□□ XML□□ □□□□ □□□(CVSS □□, □□□ □□ IP)□ □□□□ □□□ □. □□ □□ XSIAM□ □□□ □□□ □□□ □□□□□ □□□ □□□ □ □□□□. □□ B□ syslog□ □□ XML □□□ □□□□□ □□□□ □□ □□□□ □□□□. □□ C□ □□□□□□ □ XSIAM□ □□ □□□□ □□ □□□ □□□□□. □□ D□ □□□□ □□□ □□□□□ □□ □□ □□□□. □□ E□ □□□□ □□□□ □□□□.

NEW QUESTION: 19
Cortex XSIAM□ Cloud Identity Engine□ □□□ □□□□ □□□□□ □□□?
A. Cortex XSIAM□ □□ □□□ □□; □□□ pan_dss_raw □□□ □□□ □□□□ □□□ □ □ □
B. Cortex XSIAM□ □□ □□□ □□; □□□ □□□□□ □□□ □□□ □□□□ □□□ □ □□
C. Cortex XSIAM□ □□□ □□□ □□; □□□ pan_dss_raw □□□ □□□ □□□□ □□□ □ □□
D. Cortex XSIAM□ □□□ □□□ □□; □□□ □□□□□ □□□ □□□ □□□□ □□□ □ □ □
Answer: C (LEAVE A REPLY)
□□ □□ □ □□□ □□□ □□□ □□ Cloud Identity Engine□ Cortex XSIAM□ □□□ □□□ □□□□□ □□□. □□ □□□ □□ □□□□ □□□ □□□ □□□□ pan_dss_raw □□□ □ □□ □□□□ □□ □□□ □□□ □ □□□□.

NEW QUESTION: 20
□ □□□□ □□ □□□□□ □□ □□□ □□ XSIAM □□□□ □□□□□ □□□. □□□□□ □□□ □□□ □□□. 1. □□ □□ □ □□□□ □□□□ □□ □□□ IOC□ □□□□□. 2. □□ □ IOC□ □□□ □□□□ □□□□□□. 3. IOC□ □□ □□□□(□: IOC□ □□□ □□ □□□ □ □□□ □□ □□□ □□)□ □□□□□. 4. Palo Alto Networks NGFW□□ □□□□ □□ □□ IP/□□□□ □□□□ □□□□□. 5. □□□□ □□ □□□ IOC□ □□ □□ □□□ □□ □□ □ □ □□□□□ □□□□□ □□□□□. □ □□□□ □□□□ □□□□□ □□□□ □ □□□□ XSIAM □□ □ □□ □□ □□□ □□□□□? (□□□□ □□ □□ □□)
A. XSIAM□ □□ □□ □□□□□ □□□□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □ □□□.
B. □□□□□ □□ '□□□ □□'(□: □□ □□□ □ □□ □□□ IOC)□ □□□ □ □□□ □□ '□□' □□□ □□□□ □□□ XSIAM □□□□ □□.
C. NGFW □□ □ □□ TIP API □□□ □□ XSIAM 'Action' □□ □□.
D. API □□□ □□□ □□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□ □□□ '□□ □ □' □□□ □□□□□.

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

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

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

NEW QUESTION: 21

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

A. XSIAM □□□□ □□□ □□ □□□ □□ □□ □□□ □□□ JSON □□□□ □□□ □ □□ □□. □□ □□□ □□ □□□□ □□ □□ □□□ □□□□.

B. XSIAM□ □□ □ □□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□□. 'message' □ □□ □□□□□□ □□□ □□('In')□ □□□ □□□ □□□□□ □□□□ □□□ □□□□□. 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□ □□ □□ □ □□□ □□ □□□ □□ □□ □ □□□ □□□ □□ □□□□.

NEW QUESTION: 22

A. □□ A

B. □□ B

C. □□ C

D. □□ D

E. □□ E

Answer: A (LEAVE A REPLY)

XSIAM□ □□ API□ □□ □ □□□ □□□ □□ □□ □□□□□□ □□□□□. □□□ □□□ □□□ XSIAM □□□□ □□□ □□ □ □□□, □□□□ □□□ □□ □□/□□□ □□□ □□ (□□□□□ □□ □□ □□)□ □□ □□□ □□□□□□ □□□□ □□□□. □□ A□ □□□ □ □□□ □□□□□ □□□□ □□□□ API □□□□ □□□ □□□□ □□□□□(□□□ □□ □ □ □□ □□□ □□□ □ □□). □□ B□ XSIAM □□□ □□□□ □□/□□□ □□□ □□ IdP □□□ □□□ □□□□. □□ C□ □□□□□ □□ □□□□ □□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□. □□ D□ □ □□ □□ □□ □□□ □□(□□ □ □□□)□□ □ □□□□ □□ □□ □□□□□□ □□□□□. □□ E□ □□□□□. XSIAM□ □□□ API□ □□□ □□□ □.

NEW QUESTION: 23

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

A. _□□□_□□

B. _□□_□□

C. _□□□_□□

D. _□□□□_□□□

Answer: (SHOW ANSWER)

□□□ □□ □□□ □□□ □ _event_type □□□ □□□ □□□□ □□□ □□□ □□ □□□□ □. □□ □□ Cortex XSIAM □□□ □□(XDM)□ □□ □□□□ □□□□ □□□□□.

NEW QUESTION: 24

□ □□□ □□□ □□□□□ □□□□ Palo Alto Networks Cortex XDR□, □□□□ □□ □□□ □ XSIAM□ □□□□ □□□□. □ □□□ XDR□□ □□□ □□□ □□□□□□ □□□□, □□ □ □□□□□ □□ □□ □□□□ □□ XSIAM □□□□□ □□□□ □□□□□ □□□□□ □□ □. □□□ □□□ □□ □□(Windows, macOS, Linux)□□ □□ □□□ □□□ □□□□□ □□ □□, XSIAM □□□□□ □□ □□ □□□□□ □□□ □□□□□ □□ □□□□. □□ □□ □□ □ □□ □□□□□ □□□ □□□ □□□ □□□ □□□□ □□□□, XSIAM □□□□ □□□ □ □□ □□□□ □□ □□□ □□□□□?

A. XDR□ XSIAM□□ □□□ □□ □□□ □□□□□ □□□□□. □□□ □□□ □□ □□□□ XSIAM □□□□□ '□□ □□'□ □□□□ □□□ □□ XDR □□ API□ □□□□□. □□□□□ □□ □□ □□□□ XDR API□ □□ □□ XSIAM □□□□□□ □□□□□ □□□□ □□□□□

□□□□ □□□□□. □□ □□: XSIAM□□ XDR API□ □□□ □ □□□ □□ API □□ □□□ □□□□□.
B. XSIAM □ □□ Cortex XDR □□□ □□□□□. XSIAM□ XDR □□ □ □□□□□ □□ □□ □□□. XDR □□□□□ □□□□□ XSIAM □□□□□ 'Cortex XDR - □□□□□ □□' □□□ □□□□□. □□□ □□ □□□□□ 'Cortex XDR - □□□□□ □□ □□ □□□□' □□□ □□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□□ XSIAM □□□□ □□□ □□□□□□□. □□ □□: □□□□ □□□ □□ □ □□□□ □□□□□ □□ □□□ □□□□ XDR □□□□□ □□ □□□□ □□ □□□□ □□□□ □□□.
C. XSIAM□□ □□□ □□□□ □□□ □□ □□□□□ □□□□ '□□ □□'□ □□□□ □□□ □□. □ □□□□□ XDR API□ □□□□ □□□□□□ □□□□□. □□ □□□ □□, XDR□ SFTP□ □□ □□□□□ □□ □□□□□ □□□ □□□ XSIAM□□ □□□□□. □□ □□: □ □□□ □□ □ □□□ □□□ □□□□ □□ □□□ □□□□□.
D. XDR □□□ □□□ □(□: Kafka)□ □□□□□. □□□ □□ □□□□□□□ Kafka□□ □□ □□ □□□□ XDR API□ □□ □□□□□□ □□□ □, XSIAM Ingest API□ □□ □□ □□ □ □ □□□□ XSIAM□□ □□ □□□□□. □□ □□: □□ □□□ □□ □□□ □□ □□□□□□ □□□ □□ □□□□ □□□□□.
E. □□ □□□ XDR □□□ □□ □□□□□□ □□□□ □□□□□ XDR□ □□□□□. XSIAM □ □□□ □□□ □□□ □□□ □□□□□. □□□ □□ XSIAM□ XDR□ □□ □□ □□□□□ □□□□□. □□ □□: □□ □□□ □□ XSIAM□ □□□ □□□□□ □□□ □□□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)
□□ □□□□□ □□□ □□□ □□□ □□□ □□□□ Cortex XDR□ XSIAM □□ □□ □□□ □□□□□. XSIAM□ XDR □□ □ □□□□□ □□ □□□□ □□□□ □□ □□□ □□□ □□ □ □□□□□. XSIAM □□□□□ 'Cortex XDR - □□□□□ □□' □ 'Cortex XDR - □□□□□ □□ □□ □□□□' □□□ □□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□. □□□□□ □□ □□ □□□□ API □□□ □□ □□□ □□ □□(□: □□□□□□ □□□ □□□□ XDR □□□□□ □□□□ □□ □□), □□□□ □□□ □□ □□□ □□, □□□ □□ □□□ □□ □□ □□□ □□□□□. □□ □□□□□ □□□ □□□ □□ □□□ □□□□□ □ □ □□□ XSIAM □□□□ □□□ □□□□ □□□□□ □□ □□□. □□□ □□ □□□ □□□ □□□ □□□□□ □□□ Palo Alto Networks □□□□ □□□ □□□□□□.

NEW QUESTION: 25
Palo Alto Networks NGFW□ □□□□ □□ □□□□ □□□□ XSIAM □□□ □□□ □□□□ □. □□ □□□ □□□□□ □, □□□ □□□□ □□□ □□ □□□□□□□ □□ XSIAM□ 'app_id' □□□ '□ □ □□'□□ □□□□□. □□□□□ □□□ □□ □□□ 'app_id'□ □□□□ □□□□ □□□□□. □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□□□□ □□ □□□ □□□ 'app_id' □□ □□□□ □□□ □□□□□□, □□ XSIAM □□ □□ □□□ □ □□ □□□□ □□□□.
B. Palo Alto Networks NGFW □□□ XSIAM □□□ □□ □□□ □□□□□□ □□□ □□□ □ □ □□□ □□□□□ □□□□□□ □□□.

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

□□ □□ □□□□ □□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□□ □□ □□ □□ □□□□□. □□ □□□□□ □□ □□ □□□ □□□□□ □□□□ □□□. XSIAM□ □□ □□ □ □□□□ □□□□□ □□□. □ □□ □□□ □□□□□ □□□□□ □□ XSIAM □□ □ □□ □□□ □□□ □□□ □□□□ □□□?

A. '□□ □□□□' □ '□□□□ □□' □□□□□□ □□□□ □□□□ □□□ □□ □□□□ PDF □□□□ □□□□□.

B. □□□ □□□ □□□□□ □□□□ '□□ □□' □□□□ □□□□ □□ □□ □□□ □□□□ □□.

C. □□ □□ □□□ □□ IP□ □□ □□□□ □□ □□□ □□□□□ □□□□□ □□ □□□□ □□□□ □□□ □□ □□ □□□□ □□□ □□□□ XQL □□ □□ □□□ □□ □□ □□□□ □□□□. PDF □□ CSV □□□□ □□ □□□□ □□□ □□□□□.

D. '□□ □□' □□□□ □□□□ □□□□□ □□ □□ □□□ □□□ □□□□□.

E. API□ □□ □□□ □□□□ □□□□ □□□□ □□ XSIAM □□□□ □□□ □□ □□□□□ □□□□□.

Answer: C (LEAVE A REPLY)

□□ □□ □□□ □□ □□□□□ □□ □□□ □□ □□□□ □□□□□□ □□ □□□ □□□ □ □□□ □□□□□. □□ C□ □□ □□□□□ □□□ □□ □□□□□. XSIAM□ □□□ □□ □□□□ □□□□ XQL □□□ □□□ □ □□□□. network_connection_logs □□□ □□ □□/□□ IP □ □□□□□ □□□ □□□□ □□ □□ □□□ □□□□□. □□□ □□ □□ □□□□ □□□ □□□□ □□ □□□□□ □□ □□□□ □□□□ □□□□ □□□□□. □ □□□□ □ □□□ PDF □□ CSV □□□□ □□□□ □□□ □ □□□ □□□ □□□□□. □□ A□ E□ □ □/□□ □□□□□□, □□ B□ D□ □□□□□ □□ □□□ □□□ □□□ □□ □□□ □□□ □ □□ □□□□ □□□□.

NEW QUESTION: 28

XSIAM□ □□□□□ □□□ □□□ □□ □□ □□□(ICS) □□□□□□ □□□ □□□□ □□ □. □□ □□□□ □□ □□ □□□□□□ ICS □□□□□ □□ □□□□ □□□ □□□ □□□ □ □□□□. ICS □□□□ Syslog(UDP)□ OPC UA □□□□ □□□□ □□□□□. XSIAM□ □ □□ □□□□ □□□ □□□□□ □□□ □□□ □□□□□ □□□□ □□□ □ □□ □□□ □ □□□□?

A. ICS □□□□ □□ □□ XSIAM □□□ □□□□ □□□□, □□□ □□□□□ □□□□ □□ XSIAM □□□□□ □□□ □□□ □□□□ □□□□□ □□□ □□□ □□□□□.

B. ICS □□□□□ USB □□□□□ □□□ □□□□□ □□□□, □□□□□ □□□ □□ □□ □□□□□ XSIAM □□□□ □□□□ □□□□□ '□□□ □□□□'□ □□□□□.

C. ICS □□□□ □□ □□□ □□□ □□□□ □□□ □□□ □□, □□ □□□ □□□ □□ □□ □□□□□ □□ □□ □□□□ VPN □□□ □□□□□.

D. XSIAM□ □□□ □□ □□□ □□ □□□□□ ICS □□□ □□□□□□ □□□□ □□□ □□ □□ □□□□ □□□ □□□□ □□□□ □□□ □ □□□ □□□□□.

E. □□□ NAT □□□ □□□□ □□ □□□□□ □□□ □□□□ DMZ□ □□□ XSIAM □□□ □ □□□ □□ □□□□□ □ ICS □□□ □□□□□.

Answer: A (LEAVE A REPLY)

□□□ □□□ □□ □□□ □□ □□□ □□□ ICS □□□□□ □□, □□□ □□□□(□□ □□ □/□□□□ □□□□ □□□ □□)□ □□ □□□□ □□□ □□□□ □□□□□. □□□ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□ ICS □□□□□□ □□□□ □□□ □□□□ □ □□ □□□ □□□□ □□□ □□□ □ □□□ □□□. □□ □□□□ □□ □□□ □□□□□(C, E), □□ □□□□□□□ □□□□□□(B), □□□□ □□ □□□□□ □□□ □□□□□(D).

NEW QUESTION: 29

XSIAM □□□□□ □□□□ □□□ □□ □□□ □□□□□ □□□ □□ □□ □□□ □□□□ □□□□. □□ □□□ □□ □□ IP□□ 60□ □□ 5□ □□□ □□□ □□ □□□ □□□ □□ □ □□ □□□□□. □□□ SOC□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□ □□ □ □□ □□(□: '□□□', '□□')□ □□□□ □□ □□□ □□ □□□ □□□□□ □□□. XSIAM □□□□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □ □□ □□□ □□□ □□□ □□□ □ □□□□?

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

B. □□ □□ □□□ □□□□ □□ □□□ □□□ □□ 'OR' □□(□: '□□□ □□ = '□□□' □□ □□□ □□ = 'root')□ □□□□ □□ □□□ □□ □□□□ □□□□.

C. □□□ □□ □□ □□ □□□ □□□ □□□ 'target_user' □□□ □□ □□□ □□ □□ □□ □□□ □□□□□ □□□□ □□□ □□ □□□ □□□□□. □□□□ □□, □ □□ □□□ □□ □ □□ □□□ □□ □□□ □□□.

D. □□ □□□ □□ □□□ □□ 60□ □□ 30□□ □□□ □□□ □□ □□ □□□ □□ □□□ □ □□□□ □□□□.

E. □□ □□□ □□□ □□ □□□ 5□ □□ □□□□ □□ □□□ □□□□□ □□□□.

Answer: C (LEAVE A REPLY)

□□ C□ □□□□□ □□ □□□ □□□□ □□ □□ □□□□□ □□ □□□ □□□□□□. □ □□□ □□□ □□□□ □□□□□ □□ □□□ □□□□□ □□□□ □□□□ □□□ □□□ □ □(□□ □□ □□ □□)□ □□ □□ □□□ □□□□ □□□ □ □□□□. □□ □□ □□ □ □□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□. □□ A□ B□ □□ □□□ □□□□□ □□□□ □□□□ □□□□. □□ D□ □□ □□□ □□□□□ □□□□□. □□ E□ □□ □□ □□□ □□, □□ □□ □□ □□□ □□□□.

NEW QUESTION: 30

□ □□□ □□ JSON □□□□ □□□ □□□□ □□□ □□□□□□□ □□□□ □□□□. □ □□□ Broker VM□ □□ □□□ □□□ Cortex XSIAM□□ □□□□ □□□. JSON □□□ □□ □□ □□□ □□□ □□□ □□□□□. XSIAM □□□ □□□ □□□ □□□ □□ □□ □ □□□ □ □□□□ □□ Broker VM□ □□□ □□□□ □□□ □□□□, □□ □□ □□□ □□ □□ □ □□ □□ □□□ □□□□□?

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

B. □□□□□□□ HTTPS□ □□ JSON □□□□ Broker VM□ XDR □□□□ □□□ □□□ □ □, Broker VM□ JSON □□□ XSIAM □□□□ □□□□ □□□□□.
C. □□□ VM□□ Universal Data Collector□ □□ 'HTTP □□□'□ □□□□□, JSON □□□□ □□ □□ □□□□□□ □□□□, Cortex XSIAM □□ □□□ JSON□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□□.
D. syslog □□ HTTP□ □□ Broker VM□□ □□□□ □□ □□□□□□ □□□□ □□□ □□ □□□□□ □□□□ □□ JSON□ CEF □□□□ □□□□□.
E. XSIAM API□ □□□□ □□□ VM□ □□□ □□□□ JSON □□□ □□ □□□□ □□□ □ □□□□ □□□□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
□□□ □□ JSON □□□ □□, Broker VM□ Universal Data Collector□ 'HTTP Listener'(C)□ □ □□□ □□□□□□□ □□□□ □□□ □ □□ □□□ □□□□□□ □□□ □ □□□□. □□ □ □□ JSON□ □□□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□. □□□ Cortex XSIAM □□(□□□ □□□ □□□) □□ '□□ □□'□ □□□□ □□□ JSON □□□□ □ □ □□□ □□□□□ □□□□ □□□□□ □□□. □□ A□ XSIAM□ □□ □□ □□ □□□ syslog□□ □□□ JSON□ □□□□ □□□□ □□□□ □□□□ □□□□. □□ B□ □□□□ □□□□. XDR □□□□ □□□ □□□□ □□□□□ □□□ JSON □□□□ □□□□. □□ D□ □□□ □□□□□□ □□□□□□ □□ □□□□ □□□□□ □□, XSIAM□ Broker VM□ □□ □ □□□ □ □□□□. □□ E□ Broker VM□ □□□□□, □□ □□ □□□□□□□ □□□ □ □□□ Broker VM□ □□ □□□ □□□□□□ □□ □□ □□□□ □□□□.

NEW QUESTION: 31
XSIAM □□□□□ □□□ □□ IP□ □□ □□ □□□ □□□□ □□ XQL □□ □□ □□□ □□ □□ □□□□. □□ □□□ □□ □□□□□□ □□□ □□□ □ □□ □□□ □□□□□ □□ □ □□□□□. □□ □□□□□ □□ □□ IP □□□ □□□□ □□□□ □□□□□□□□ □□ □ □□□ □□□□. □□□ □□□□ □□ □ □□□□□□□ □□ □□ □□□ □□□ □□□ □□ □□□?
A. □□□ □□ □□□□ □□□ □□ □□□ □□ □□ □□ □□□. □□ □□□ □□ □□□ □ □ □□□□□ □□ □□ □□□□□ □□□□ □□ □□□ □□ □ □□ □□□□□.
B. □□ □□□ □□□□□ □□ □□□□ □□ □□□□□ □□ IP □□ □□□ □□ □□□□ □ □□□ □□ □□ □□□ □□□□□.
C. □ □□□□ □□□ □□ □□ □ □□ □□ □□□ □□□ □□ □□□□□□□ □□ □ □□ □□□ □□□□ □□□□. □□ □□ □□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□ □ □ □□□□.
D. □□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□ □□□□□ □ □ □□ □□□ □ □□□□□ □□□ □ □□□□.
E. □ □□□□□□□ □□□□ □□ □□ □□ □□□ IP □□□ □□ □□□ □□ □□□ □□□ '□□' □□□ □□□ □ □□□□.
Answer: C (LEAVE A REPLY)

□□ C□ □□ □□□ □□□□ □□□□□. □□ □□□ □□□□ □□□□ □□□□ □□ □□ □□ □□□ □□□ □□□□□. □□ □□□ □□□□□ □□ □□□ □□□□ □ □□□ □□□ □□□. □□ □□□ IP □□□ □□ □□ □ □□□ □□□ □□□□ □□ □□ □□□ □□ □ □ □□□ □□□□ □□□ □□ □□□□ □□ □□ □□□□□□. □□ □□ □□□ □□ □□□□ □□□ □□ □□□□ □□□ □□□ □□ □□□ □□□□□ □□ □□□ □□ □□□□ □□□ □□ □□ □ □□□□. □□ A: □□□□ □□□ □□ □□□ □□ □□ TI □□□□ □□ □□□ □ □□□□. □□ □□ □□ □ □□ □□□ □□/□□ □□□□ □□□□ □□□□□. □□ B: □ □□□ □□□ □□ □□ □□□ □□□□□. □ □□□ □□□ □□ □□ □□□□ □□□□□ □ □ □□□ □□ □□□ □□□ □□□ □□□□ □□□□. □□ D: XSIAM□ □□□□□ □□□, □□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□ □□ □□ □ □□□□ □□□□. □□ E: □□ □□□ □□□ □□□□□□□ □□□□□ □□ □□□ □□ □□ □□□□. □□□□ □□□ □□□□ □□□□ □□□□□ □□□ □□ □□□ □□□□□.

NEW QUESTION: 32
□□□ APT □□□ DNS □□□□ □□□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□. □□□ □□□□□ □□□□ □□□ □□□ DNS □□ □□ □□□□ □□□□□ □□ □□ □ □ □(C2) □□□□□ □□□□□, □□□ □□□□ □□□□ □□□□□□ □□□□□□□□□□ □ □ □□□□ □□□□. XSIAM□□ □□ □□□□□ □□ □□□□□ BIOC □□□ □□□□ □□ □. □ □□□ □□ DNS □□ □□□ □□ □□□ □□□□ □ □ □□□ □□□□□ □□□□□ □ □□ □□□□ DNS □□□ □□□ □□□ □□□. □ BIOC□ □□ □□(false positive)□ □□ □□□□ □□ □□□□ XSIAM XDR □□□ □□ □□□ □□□ □□□□□?
A.
B.
C.
{<□>}:
D.
Answer: C (LEAVE A REPLY)
□□ C□ DNS □□□□ □□□□ □ □□ □□□□□ □□□ BIOC□□□. □□ A□ □□□ □□ □□□□ □□□□, □□ □□□ □ □□□□. □□ B□ □□ TXT □□□□ □□ □□□ □□□□ □, □□ □ □□ □□□□□ □□□□ TXT □□□□ □□ □□□ □□□□ □□□□. □□ D□ □ □ □□□□□. □□ E□ □□ □□□ □□□□ □□□ □□□ □□□, □□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□ □ □□□□. □□ C□ □□ □□ □□□ □□□ □

□□□□. □□□□□ 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)

□□□□□ □□□□ Cortex XSIAM □□□□□ □□□□ □□□□□. □□□□□ □□□□□ □ □□ □□□ □ □□□□, □□□□□ □□□□□ □□□ □□□□ □□□□ □□□□ □□□ □ □□□ □□□ □□□□□.

NEW QUESTION: 37
□□□ □□□ □□ □ □□□ XSIAM□ □□□□ □□□, □□ □□□□ □□□ □□ □ □□□ □□□□ □□ □□ □□□□ □□ □□□□ □□ □□□□□ □□□□ □□□. □□ □□□□□ □□ 7□ □□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□□ □□ □□□ □□□ □ □ □□ □□□ XSIAM □□□□ □□ □□□ □□ □□ □□□ □□□□□?
A. XSIAM □□□ □□□(CDL) □ □□ □□ □□□ □□□ □□□ □□□ □□ □□.
B. XSIAM□ □□ □□ □□□ □□□ □□ □□ □□ □ □□ □□□ □□□□□.
C. XSIAM□ □□ □□(XAE)□ □□□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□□□.
D. XSIAM □□□ □□ API□ □□□□ □□ □□ □□ □□ □□□□□□ □□□ □□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.
E. XSIAM□ SOAR □□□□□ □□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
□□ □□ □□□ □□□ □□□, □□□, □□□ □□ □□□□□. Cortex Data Lake(CDL)□ XSIAM□ □□ □□□□ □□□□, □□□ □□□ □□□□□ □□□□□. CDL□ □□□ □□□ □□ □□ □□□□□□, 7□ □□ □□□ □□□□□ □□□□ □□ □□□ □□ □□(A)□ □□ □□□. □□ □□ □□(B, C, D, E)□ □□ □□□ □ □□□ □□□ □□□ □□□ □□□, □□ □□ □□□□ □□□ □□□□ □ □□ □□□□□ □□ □□□ CDL□ □□ □ □□□ □□□□. XSIAM□ □□ □□ □ □□ □□□ CDL □□□ □□□□ □□□ □□□□ □□□□□. CDL □□ □ □□□ □□□ □□ □□□ □□□ □□□ □□□ □ □□□□.

NEW QUESTION: 38
□□□□ □□ □□□□ □□ □ □□□□□□ □□□□ □□□□□ □□□ Cortex XSIAM□ □□ □ □□□□□ '□□□□□ □□' □□□ □□□□ □□□ □□□□. □□□□ □□ □□□ '□□ □ □ □ □□'□ □□□□□. □□□□ □□ □□ □□□ □□□□ 'Cortex XDR - □□ □ □□□□' □□ □□□□ □□□ □□□ '□□: □□□ □□ □ □□' □□□□ □□□□□. □□□ □□□ □ □ □□□ Cortex XDR□□ □□□ □□ □□□□ □□□ □□□□□. □ □□ □□□ □□ □□□ □□ □ □□ □□ □□□ □□□□□?
A. □□ □□□□□□ XSIAM □□□□□ □□□□ □□□□□ Cortex XDR□ □□□ □□□□ □ □□□.
B. □□□□□ '□□□ □□' □□□ □□□ □□ □□□(□: □□□□ ID □□ □□□ □□)□ □□ □□ □□□□.
C. XSIAM□ Cortex XDR □□□□ □□□□□ □□ □□□ □□□ □ □□ □□□ □□□□.
D. XSIAM □□□ Cortex XDR API □□□□□ □□ □□□ □□□□ □□□□ □□□□ □□□ □.
E. XSIAM □□□□ □□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□□□.

Answer: (SHOW ANSWER)

XDR□□ □□□ □□□ □□□ □ '□□□ □□ □ □□' □□□ □□□□ □□ □□□□ □□□ (B)□ □□□□ □□□□ □□□□□. □□□□□ □□ □□□ □□□ □□□□ □□□ □□ ID(□: □□□□ ID)□ □□□□□. □□, XSIAM□□ □□□□ □□ □□□ Cortex XDR□□ □□ □ □□□□ □ □□□ □□□ □□ □□, API □□□ □□□ □□□(C)□ □□ □□□□□. □□□ □ □□□□(A)□ □□□□□ □□ □□□ □□□ □□ '□□□ □□ □ □□'□ □□ '□□□ □□ □ □ □□' □□ '□□□□ □□□□' □□□ □□□□□□. □□□ □□(D)□ □□□□□ API□□ '□□□ □□ □ □□'□ □□ □□ □□ □□ □□ □□ □□□ □□□□□. □□□□ □□ □□(E) □ □□□□□ □□ □□□ □□ '□□□ □□ □ □□' □□□ □□ □□ □□□□□ □□□□ □ □□□□ □□□□ □□□ □□□□□.

NEW QUESTION: 39

□□□ XSIAM□ □□ □□ □□□□□ □□ '□□ □□(Chain of Custody)' □□□ □□□□ □□, □ □□□□ □□ □□ □□□ □□□ □□□□□, □□ □□□, □□□□□ □□□□□ □□□ □ □□ □□□□□ □□□. □ □□□□ XSIAM□ □□ □□ □ □□□□ □□ □□ □□□□ □□□ □□ □□□ □ □□□□. □□ □□□ □□ □□□□ □□□□ □□□□□ □□□□ □□ □□□ □ □ □□□ □□□□ □□□ □□□□ XSIAM □□□□ □□□□ □□□□ □□□□□□.

A. □□□ □□□ □ □ □□□ □□□□ '□□ □□' □□□ □□□□□.

B. □□□ □□ □□□□ □□□□ □□□ □□□□. □ □□ □□□ XQL □□□ □□□□ □□□ □□ □□□ □□□□□(□□ □□ □ □□□□ □□□ □□ '□□' □□ □□ □□). □□ □□ □□ □□□□□, □□ □□ □□, □□□ □□□□ □□□□ □□□□ □□□□□. '□□ □□□' □□ '□□□'□ □□□□ □□ □□□ □□□□ □□□□□.

C. □□ □□□□ □□□□ '□□ □□' □□□□ □□□□ □□ □□□□□□□ □□□□□.

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

E. SOC □□□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□ □□□□□□ □□□□ □.

Answer: B (LEAVE A REPLY)

XSIAM □□□□ □□□□ □□□ '□□ □□(Chain of Custody)' □□□ □□□□ □□□ □□□ □□, □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□ □□□ □□ □□□□ □□□□ □ □□ □□□ □□□□. □ □□□□ □□ XQL □□(□□□ □□ □ □□□□□□ □□ □□ □□ □□ □□)□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□□□. □□ □□□ □ □ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□. □□ A, C, D, E□ □□□□□ □□□□□□, □□□□ □□ □□□ □□□ □□□□□ □ □□□ □□ □□□□ □□□□.

NEW QUESTION: 40

□ □□ □□□ XSIAM□ □□□□ □□□, □□□□ □□□□ □□□ □□ □□□□ □□□□ □ □ □□□ □□ □□□ □□□ □□□□. □ □□□ □□ □□□ □□□□ □□□ □□ □□□□ □ □ □□□□□□ □□ □□□□□ □□ □□□□□□. CISO□ □□□□□ □□ □□□ □□□ □ □□□ □□□ □□ □□ □□□ □□□□, □□ □□ □□□ □□ □□□□□ □□ □□ □□□ □

□ □□□ □□□ □□□□ □ □□□ C2 □□□ □□□□□ □□□ □□□□□. □□ XSIAM □ □ □□(□□ □□ □□) □ □ □□ □□□ □□ □ □□□□ □□ □□□□□?

A. □□ A

B. □□ B

C. □□ C

D. □□ D

E. □□ E

Answer: C (LEAVE A REPLY)

□□ C□ □□ □□□□□ □□□□ □□ □□□□□. A□ B□ □□□□□ □□ □□□□□, □□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□□□□. □□□ □ □□□ □□□□□ □□□□ □□ □□ □□ □ C2 □□□ □□□□□, □ □□□ □□(□□□ □ □□□□□ □□ C2 □□ □ □□□)□ □□□□□. XSIAM□ '□□' □□□(□□ □□ □□□ □□□)□ □□ □□□ □□ □□□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□ □□ □ □□□ □□ □□□□□ □□□ □□ □□□ □ □□□□. □□ D□ □□□ □□ □□□ □□□ □□□□ □□ XSIAM □□□□ □□□ □□ □□□ □□□□. □□ E□ □□□ □□ □□□□□, □□ □□□□ □□□□□ □□□ □□ □□□□ □□□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□, □□ □□□□ □□□□ □□□□.

NEW QUESTION: 41

□□□ □□ □□□(MSSP)□ □□□□ □□ □□□ □□ □□□ □□□ □□□□ XSIAM□ □□ □□ □□□ □□□□□. □□ □□□□ □□ □□□ XSIAM □□□ □□□□□. MSSP□ □□□ □□□ □□, □ □□□□ □□ □□, □□□ □□□ □ □□□□ □□□ □□□ □□□□ □□□. □□□□ □□□□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□□, □□□□ □□□ □ □□□□?

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

B. □□□ □□□ □□□ □□□ □□□□ □□□ □□ □□□□□□□ □□□(HCI) □□□□ □ □□□ □□□□ □□□□□ □□□□□. □□□□ □□□□ □□□ □□□□□ '□□□ □□' □ □□ □□□ □ □□□□.

C. □□ □□ □□□ Kubernetes□ □□ □□□□ □□□□□□□ □□□□ □□□□ □ □□□□ □□ □□□□ □□□ □□□ □□□□□ □□ □□□□ □□ □□□ □□□□□ □□□ □□□ □.

D. □□ □□□□ □□ □□ □□ □□□ □□□□□ □□ □□□ GPU □□□ □□□□□, □□ □□□ □□ □□ XSIAM □□□□□ □□□ □□□□□□ □□□ □□□□.

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

Answer: B (LEAVE A REPLY)

□□ □□□ XSIAM□ □□□□ MSSP□ □□, □□□□□ □□□ □□□□□ □□□□ □□□ □□□ □□ □ □□ □□□ □□□□ □□ □□□□□. □□ □□ □□□ □□□(A). HCI(B)□ □ □□ □□ □□□ □□ □□□□□. HCI□ □□ □□□□□□ □ □□□□ □□ □□□ □□ □□

□ □□□□ □□□ □□□□ □□□□□ □ □□□ □□□ □ □□□ □□□□(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□ □□□□ □□□ □□□□□ □□ □□□ □□□□□ □□□□□ □□□□ □□□□ □ □ □□□□ □□□□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□□□ □□□□ □□□

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

NEW QUESTION: 43
XSIAM □□□□□ Linux□ □□□□ □□ □□□□□ □□□□ □□□□. □ □□□□□ □□ □ □□ □□□□ □□□□□ □□□ □□□□□ □□□□□. □□□ XSIAM □□□□ □□ □□□□ □□□ □□□□ □□□□□ '□□ □□' □□ '□□□ □□' □□□ □□ □□□□□ □□□□□.
□□ □□, □□ □□□ □□ □□ URL□□ □□□ □□□□□□ □□□□ □□□ □□□□□ □ □ □□□□ URL□ □□□□ □□□ □□□□□□. □□ □ □ □□□ □□ □□□ □□ □□□ □ □□□, □□□□ □□ □□□ □□□□□?
A. □□ □□□ □□□□□□□. XSIAM □□□□ □ □□□ □□ □□□□ □□□□□ □□ □□ □□□.
B. XSIAM □□□ 'Production_Linux' □□□□ □□□ □□□□. □□□ □□□□ □□□□□ □ □ □□□□□.
C. □□□□□ □□□ XSIAM □□□□ □□/□□□□□ □□□ □□□□ □□□□. □□ □□□ □ □□□ □□□ □□□ XSIAM □□□□ □□□□□ □□□ FQDN□ □□□□□ □□□□ □□ □.
D. XSIAM □□□□□□ □□□□□ TCP □□ 443□ □□□□ □□□□ □□□□ □□□□. □□ □□□□ URL□ □□ □□□□ □□□□□.
E. Linux □□□ □□□ XSIAM □□□□□ □□□□□ □□ SSL □□□ □□□ □□□ □□□□ □□. □□□ NTP□ □□□□□□.
Answer: (SHOW ANSWER)
□□ C□ □□ □□□ □□□ □□□ □□□□ □□□□□ □□□ □ □□ □□ '□□ □□' □□ '□□□ □□' □□□ □□ □□ □□□□ □□ □□□ □□□□□.Cortex XSIAM □□□□ □□ □ □□□ □□(□: □□, EU, □□□ □□□)□ □□□□□□.□□□□ □□□ □□ □□□ □□ □□ □ FQDN□ □□□□□ □□□□□.□□□□ □□ □□ □□ □□□□□ □□ □□ □□□ XSIAM □□□□ URL(□: 'us.xdr.paloaltonetworks.com' □□ □□ *cloud.xdr.paloaltonetworks.com)□ □□□ □□□□ □□ □□□ □□□□□□ □□ □□□ □□ □ □□□□□.□□□□ □□ □□□ □□ □□ □□ □□□□□ □□□□ □□□□ □□ □□□ □□□□□ □□□ □□□ XSIAM □□□□ FQDN□ □□□□□ □□□□□ □□□□ □□□□. A, B, D, E□ □□□ □□□ □ □□ □□, □□□□ □□□ □□□ □□□ □□ '□□ □□'□ □□ □ XSIAM □□□□□ □□ □□□□□ □□□ □□ □□□□ □□□□□.

NEW QUESTION: 44
XSIAM □□□□□ □□□ API □□□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□ □□ □ □□□□□ □□□□. □□□ JSON □□□□□, □□ 'details' □□□□ □□□ □□ □□ □□ □□ □□□□ □□ □□□□ □□□ JSON □□□□ □□□□ □□□□. □□□ □□□ □□□ JSON □□□□ XSIAM □□□ □□□ □□ JSON □□□ □□ □□□□ □□□□. □□□ □□ □□ □□ □□□□ □□□□□□.

'event_data' □□□ □□ □□□□ □□□□□. "event_data"□ □□□ JSON □□□ □□□□□ XSIAM □□ □□□ □□□ □□□ □ □□□□?

A. □□ □□ □□□ □□□□ □□□□ 'event_data' □□ □□□ □□□□ □□□ □□, □□□ □ □ □□□ □□□□□ □□ □□□□ JSON□□ □□□□□. □ □□□ □□□□□□□.

B. □ □□□ □□□ □□ XSIAM □□ □□ □□ □□□ 'event_data' □□□ 'JSON' □□□□ □ □□□□(□□□□ □□) 'event_data' □□□ 'JSON □□□' □□□□□ □□□□ □□ □□□ □ □□□□ □□ □□□□□. □ □□ 'json_extract: event_data' □□ □□ □□□ □□□ □□□□ □□□.

C. 'event_data' □□□ □□□□ □□ □□ □□□ JSON □□□ □□□□□ □□ API □□□ □□ □□□. □ □□□□ □□ □ □□□ □□□□□, □□□ □□□ □ □□□□.

D. XSIAM □□ □□□□□□ 'mutate' □□□ □□□□ 'event_data' □□□□ JSON □□□ □□ □□□. □□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

E. 'event_data'□ □□ XSIAM □□□ □□□ □□□□□ □□□ □□□□ □□□. □□□□□□ □□□ □□□ □□ □□□ □ □□□□.

Answer: B (LEAVE A REPLY)

□□ □□□□ 'JSON □□ JSON' □□ □□□□□. XSIAM□ □□ □□□□ □□□□□ □ □□ □ □□□□ □□□ □□□□ □□□□. □□ □□□□□ □□□□ □□□ 'event_data'□ □□□ JSON □□□ □□□□□ □□□□□ □□ □□□ □□□□ □□□□. □□ B□ 'JSON □□□'□ □□ □□ □□□□□ □□□□□ □□ □□ □□□ □□ □□□ 'JSON'□□ □□□□ XSIAM□ □□ □□□ □□□ □□□□□ □□□□□ □□□□ □□□ □□□□□. □□ A□ □□□□□ □ □ □□□□□. □□ C□ □□ □□□ □□□□ □□□□□. □□ D□ □ □□□ □□ □□□ □□ □□□□. □□ E□ □□□□ □□□□ □□ □□□ □□□ □□□□.

NEW QUESTION: 45

Cortex XSIAM □□□ □□ □□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□. XSIAM □□□□ □□ AWS □□□ □□□□□, □□□ □□□□□ □□□ □□□ □□□□□. XSIAM □□□□ □ □□□ □□□ □□□□ □□□ □□□ □, XSIAM □□□ □□□□ □□□□ □□□□ □ □□□□□ □□□ □□□□ □□□ □□□□□?

A. XSIAM □□□□ □□ □□□ □□ □□□□□ HTTP(□□ 80) □□□□ □□□□□.

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

C. □□ □□, □□□ □□ □ □□□□ □□□□ □□ XSIAM □□□□ □□□ FQDN□ □□ □□ □□□ HTTPS(□□ 443) □ □□□ □□(□: Syslog, API)□ □□ □□ □□□□/□□□□□ □□ □□□.

D. □□ □□□ □□ XSIAM □□□□□□ □□□□□ □□□□ SSH(□□ 22).

E. □□□ □□□ □□ □□□ □□ □□□□□ □□ □□ □□□□ □□ □□□□□ ICMP□ □□ □□□.

Answer: (SHOW ANSWER)

Cortex XSIAM □□□ □□ □□ □□, □□□ □□, □□□□□ □□□□ □ □□□ □□□ □□ □□ HTTPS(□□ 443)□ □□ XSIAM □□□□□ □□□□□. □□, □□□ □□□ □□(□: UDP/TCP 514□ Syslog, □□□ □□ □□ □□□ API □□)□□ □□□□ □□□ □ □□□ □□

□. □□□ □□ XSIAM FQDN□ □□ □□□□ □□□ □□□□□ HTTPS □□□□ □□□ □□ □ □□ □□□ □□□□/□□□□□ □□□ □□□□□. □□ A□ HTTP□□ □□□ HTTPS□ □ □ □□□ □□□□□ □□□□ □□□□. □□ B□ □□ □□□ □□□□. □□ D□ □□□□ □ □□□. XSIAM□ □□□□□ □□□ □□ □□□ SSH □□□ □□□□ □□ □□ □□ □□□ □ □□□□. □□ E□ ICMP□ □□□ □□□ □□ □□□□□□, □□ □□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□.

NEW QUESTION: 46
XSIAM □□□□□ REST API□ □□ □□ □□ □□□□□□□□ □□□□□ IP □□□ □□ □ □ □□□□□ □□□□ □□□ '□□' □□□□□ □□□□ □□□. □ API□ □□□ □□□ □□ □□□ □□□ □□□. □□□□□ □□□□ □□□□ API □□□ □□□□ □□ XSIAM □□□ □ □□□ □□ □□□ □□□ □□□ □□□□ □□□?
A. □□□ □□ 'HTTP' □□□ □□□□, □□□□□ Python □□□□□ API □□ □□□□□□, '□□' □□□□□□ □□□□□.
B. □□□ '□□' □□□□□ □□□, '□□ API' □□□ □□□□, API □□□□□□ □□□□, □□ □□□□□ '□□' □□□ □□ □□□ '□□' □□□□□ □□□□□.
C. '□□' □□□ □□□□ XSIAM □□□□ □□ □□□□□ □□□□ API □□□ □□□□ □□ □ □□ □□□ □□□□□.
D. □□ 'VirusTotal' □□□ □□□□ □□ □□□□□□□ □□□□□ □□□ □□□□□.
E. □□□□□□ □□ API□ □□□□ □□□ □□ □□□□□□□□ □□□□□ □□□□ □□ □□ □□□ □□ '□□□ □□□'□ □□□□□.
Answer: (SHOW ANSWER)
XSIAM □□□□ □□□ □□□ □□ REST API□ □□□□ □□□□□ □□ □□□□□ □□□ □□ □□□ '□□' □□□□□ □□□□ □□□. □□ REST API□ □□ '□□ API' □□□ □□□ □□. □□ □□□□ □□ □□□ API □ □□ □□□ □□ □□□ □□□ XSIAM□□ □□□□ □ □□□ □□□ □ □□□ □□ □□□□ □□□. API□ □□□ □□□ □□□□ □□, □□ □□□ □ □□ □□□ '□□' □□□□□ □□□□ □ □□□ □□□ □□ □□□□ □□□ □□□□ □□ □□□ □ □ □□□□. □□□□(A)□ □□ □□□□□□ □□ □□□□ □□□□. □□ □□(C) □ □□ □□□□□ □□ API□ □□ XSIAM □□□□□ □□□□ □□□□□. VirusTotal(D)□ □ □ □□ □□□□□□. □□□ □□□(E)□ □□□□ □□□□□, □□□□ □□ □ □□□□ □□ □□ □□□□.

NEW QUESTION: 47
□□□□ □□□ □□ □□□ □□ □□□□□ □□□ □□□ Broker VMS□ □□□□ □□□ XSIAM □□□ □□□□ □□□□. Palo Alto Networks□□□ □□ Broker VM □□□ □□□ □□ □□ □□□□ 2.1.3 □□□□ □□ □□□□□□ □□□ □□ □□ □□□ □□□□□. □□□ □ □ □□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□ 2□□ □□ □□□ □□□□□. □□ □□ □□ □□□ □□□□ □□□□□ □□□ □□□□□ □□□□□ □□□□□ □□□ □□□ □ □□□. □ □□□□□□ □□□□ □□□□□ □□□□□ Broker VM □□□ □□□□□ □□ □□ □ □□ □□ □□□ □□□ □□□□□? (□□□□ □□ □□ □□)
A. □□□□ □□ □□□ □ □□ □□□ □□□□□ □□□ □□□ □□□□ □□ □ □□□ □□ □□ □□ □□ □□□ □□□ □□□ VM □□□ □□□□ □□ □□□□□□□.
B. □□□□□ □□□□ □□ □ □□□ VM□□ XSIAM □□□□ □□□□ □□□□ □□□□ □ □ □ □□□ □□□ □□□□, □□ 2.1.3 □□□ □□□ □□ □□□ FQDN □□ □□□ □□□ □□□□□.
C. □ □□□ □□□ □□□ □□□ VMS□ □□□□ □□□□□(□: □ □□ □□□) □□□□□ □ □□□□ □□□ □□□ □□□□ □□□ □□□ □□□□□□.
D. □□□ □□ □□□ □□□ □□ □□□□ □□□ □ □□□ □□□ □□□□□ □□□□ □□ □□□ VM □□□ □□□□ □□ □□□ □□□□ □□□□.
E. □□□□ □□□□ □ □□□ □□□ □□□□ □□ □□□ VMS□ □□□□ □□ XDR □□□ □□ □□□□□ □□□□□□ □□□□□ □□□□□ □□□□ □□ □□□□□□.
Answer: A,B,C,D (LEAVE A REPLY)
□ □□□ □□□ □□□□ □□ □□□□ □□□ □□ □□□□ □□□ □□□□□. A: □□□/□ □□ □□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□□□□ □□ □□ □□□□□. □ □ □□□□ □□ □□ □□□ □ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□□□ □ □ □□□ □ □□□ □□□□ □□□□□. B: □□□□ □□ □ □□□ □□□ □□□□ □□ □□ □□□□□. □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□□ □ □□□, FQDN/□□□ □□ □□□□ □□□ □□ □□□□ □□□□ □□ '□□□□ □□' □□□ □□□ □ □□□□. C: □□ □□□ VMS□ □□□ □□□□□ □□□□□ □□□□□ □ □□□□□□. □ □□ □□ □ VM□ □□□□□□ □□ VM□ □□□ □□□ □ □□ □□□□ □□□ □□□ □□□□□. □ □ '□□ □□□□' □□ □□□ □□□□□ □□□□□. D: □□ □ □□□ □□□ □□□ □□ □ □□□□ □□□□□. □□□□□ □□□□ □□□ □□, □□□□□ □□□□ □□ □□ □□ □ □ □□□ □□□ □□□, □□□ □□ □□□ □□□ □□□□□□. E: XDR □□□□□ □□□□ □ □□□□□□ □□ □□□ □□□□□. □□□□ □□□ □□□□ □□□ □□□ □□□ □□ □ □ □□□□. □□□ □□□ □□□□ □□ □□□ □□□□□ □□□□. □□ □□□ VMS(C) □ □□□□ □ □□□□ □□□ □□□ □□□□□.

NEW QUESTION: 48
□□ □□□ □□□□ □□□□□□ □□□□ XSIAM □□□□ □□□ □□ □□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□ □□□□□ □□, □□ □□□□ □□ □□ □□□ □□ □□ □ □ □□□ □□□ □□(false positive)□ □□□□ '□□ □□: Critical_Exploit_Attempt_CVE-2023-XYZ'□□ □□□ □□□□□ □□ □□□□□□. XSIAM□

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

A. □□ □□ □□□ □□□ □□□ □□□□□ 'Critical_Exploit_Attempt_CVE-2023-XYZ' □□□ □□□□ '□□'□ □□□□.

B. □□ '□□ □□' □□ □□□ '□□'□ □□□□, 'Critical_Exploit_Attempt_CVE-2023-XYZ' □□ □ □□ □□□□ □□ □□□ □□□ □□(□: 'process_name = 'diag_tool.exe' AND 'user_name = 'admin_user')□ □□□□□.

C. '□□ □□'□□ 'alert_name = AND 'destination_port= '8080'(□□ □□□ □□□□ □□)□ □ □□□ □□□ '□□ □□'□ □□□□ □□ □□□ '□□ □□'□ □□□□□.

D. Palo Alto Networks□□ □□ □□□ □□□ □□□ □□□ 'Critical_Exploit_Attempt_CVE-2023-XYZ' □□ □□□ □□□□□ □□□□□□□.

E. □□□ □□□□ □□ 'diagnostic_servers' □□ □□□ □□□ □□ 'Critical_Exploit_Attempt_CVE-2023-XYZ'□ □□ □□ □□□ □□□□ □□ XSOAR □□□□□ □□□□□.

Answer: B (LEAVE A REPLY)

□□ B□ □□ □□□□□□. '□□ □□' □□ □□□ '□□'□ □□□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□ □ □□□□. □□ □□ □□□ □□ □□□ □□□□□□□. □□□□ □□□ □□□ □□(□□□□ □□ □ □□□ □)□ □□□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □ □□□□. □□ A□ □□□□ □□□□□ □□□□ □□□ □□ □□□ □ □□□□. □□ C(□□ □□)□ □□□ □□□ □□ □□□□ □□, □□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□□ □□□ □ □□□□□□. □□ D□ □□□ □□ □□□ □□□□. □□ E(XSOAR □□□□)□ □□ □□ □□□□ □□□ □ □□□, □□□ □□ □□ □□□ □□ □□ □ □ □□□□□ □□□□□□.

NEW QUESTION: 49

□□□ XSIAM □□ □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□ □ □□□□□ □□□□ □□ □□□ □□□□ □□□□. □□ '□□' □□□ '□□ IP', '□□□ □ □' □ '□□ □□'□ □□□□□. □□ □□□ □□□ □□□ '□□ □□'□ '□□' □□ '□□'□ □□ □□□. □□□ '□□ IP'□ □□□ □□□ □□ □□□ □□□□□ □□, □ □□□ □□ □□□ □ □ □□□□ □□□ □□ □□□□ □□□. □□□ □□ □□ □□□ □□ □□□□ □□ □□ □□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□ □□□. □□ □□□ □□□ □□□ □□ □ □□□□?

A. □□ □, □□□ □□□ □□□□ □□ □□□ IP □□□□□□□ □□□□ 'source_ip'□□ 'country'□ 'city'□ □□□□ □□ □ □□□ □□□□□. □□, 'username'□ □□□□ 'Authentication' □□□□ □□□□ □□□ 'country' □□□ □□□□ 'failure' □ 'success' □□□ □ □□□□ □□ □□ □□□□ □□□ □□□□□.

B. □□ □□□ □□ □□□ IP □□□ □□□□ 'country' □ 'city'□ 'source_ip'□ □□□□ □□□ □ □□ XSIAM '□□□ □□'□ □□□□□.

C. XSIAM '□□□ □□'□ □□□□ 'source_ip'□ □□ □□□□ □□□□□□. □□ □□ □□ □ □□ □□ '□□ □□'□ □□□□□. □□ □□ □ 'authentication_status'□ 'failure'□□ 'source_ip'□ □□ □□□ □□□ □□□□ 'Authentication' □□□□ □□□□ □ □□□□ □□ □□□ □□□□□.
D. '□□' □□□□ '□□ □□□ □□'□ □□□□□. □ □□□□ □□ □□□ □□ □□ □□□ 'source_ip'□ 'country'□ 'city'□ □□□□□. □ □□ □□□ □□□ □□□□□ □□□□□□ □ □□□□. □□ □□, □ □□□□ □□□ □□□ □□ □□ □□ □□□ □□□□□.
E. □□ □□ □ 'source_ip'□ □□ □□□ □□□ IP □□□ □□□□ □□□ □□ XQL □□□ □ □□□□. '□□' □ '□□' □□□ □□□ □□ □ XQL □□□ □□□□ □□□ □□□ □□□ □□ □□ '□□□□ □□'□ □□□□□.
Answer: (SHOW ANSWER)
□□ □□ □□□ □□ □□□□ □□□ □□ '□□□ □□'□ '□□ □□ □□□□□ □□□□□ □ □ □□ □□ □□ □□□□ □□'□□□. □□ D: □□ □□(□□ □□ □□ □□ □□ □□ □□□ □)□ □□□ □ □□□□□ □□□□□ '□□ □□□ □□'□ □□□□ □□ □□ □□□ □□□□ □. □□□ □□ □□□□ □□□ □□□□ □□ '□□' □ '□□' □□□ □□ □□□ □□□ □□ □ □□□ □□□□□□ □□ □ □□□ □□□ IP □□ □□ □□□ □□□□□. □□□ □□ □□□ □ □□□ □□□ □□□□□ □□□□ □□□□ □□ □□ □□□□□ □□□ □ □□□□. □□ □□□□ □ □□□□ □□□ □□□ □□□□. - □□ A□ □□ □□□ □□□ IP □□□ □□□□ □, '□□'□ □□□□□ □□□□ '□□ □□ □□□□ □□'□ □□□□□. □□ □□□ □□□□ □ □□□ □□□ □□□□□ □□□ □ □□□□. □□ D□ □□ □□□□ □ □□□□□. - □□ B□ □□□ □□□□ □□□□□, □□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□ □ □□□ □□□ □□□□□□. ML □□□ □□□ □□□, □□□ IP□ □□/□□ □□□□□ □□□ □□ □□□□ □□□□. - □□ C□ □□ □□ □□ □□□ □□ □□□□□ □□□□□, □□ □ □□ □□□ □□□□ □□□□□□ □□ □□□□□ □□□□□. - □□ E□ '□□ □□ □ □□□ □□□ IP □□□ □□□□ □□□ □□ XQL □□'□ □□□□□ □□□□□. □□ '□□ □□ □□ □□ □□□'□□ □□ □□□ □□□□□ □□□□, □□□ □□□ □□□□ □□ □□□□□□ □.

NEW QUESTION: 50
□□ □□□□□ □□ □□□□□ □□□ □□ □□□ □□□□□□ □ □□□□ □□□ □□□□ □?
A. !setIncidentFields
B. !setParentIncidentFields
C. !setParentIncidentContext
D. !updateParentIncidentFields
Answer: A (LEAVE A REPLY)
!setIncidentFields □□□ □□ □□□□□ □□ □□□□□ □□□ □□ □□□ □□ □□□□□ □ □□ □□□ □□ □□□ □□□□□ □□ □ □□□□□.

NEW QUESTION: 51

XSIAM□□ □□□ □□□ □□□□ XSOAR □□□□□ □□□□□ □□□□. □ □□□□□□ □□ □□□ □□ □□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□□ □□□□ □□□ □. □ □□□□□ □□ □□□□□ □□ □□□ □□ □□□□□. XSOAR □□□□ □ □□ □□ □ □□ □ □□□□□ □□□□□ □□□□□□ □□□ □□ □□□?

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

B. □□□□ □□□ Python□ 'time' □□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□ □ □ □□ □□□ □□□□□.

C. □□□ □ □□ □□□ □□□□ □□□ □□□□□ □□ □□□□□ □□□ □□□□ □□ □ □□ □□□□□.

D. □□□□□ □ □□ □□ □□□ □□□□ □□ XSOAR □□□ □□□ CPU □ □□□ □□□ □ □□□□.

E. □□ □□□ □□ □□□ □□ □□□□□□□□ □□□□ □□□ □□ □□□ □□ XSOAR □ □□ □□ □□□□□.

Answer: A,B (LEAVE A REPLY)

□□□□□ □□ □□□□ □□□□ □□ □□ □□□□ □□, □□ □□□ □□□□□ □ □□□ □ □□□. □□ □□□(A)□ □□□□□□ □□ □□□□ □□□□ □□□□ □□□□□. Python □ 'time' □□(B)□ □□□□ □□ □□ □□□ □□□□ □□□ □ □□□, □□ □□ □□□ □□ □□ □□□□ □□□ □□□□ □ □□ □□□□□. C, D, E□ □□□□ □□□ □□ □□□□ □ □□□ □□, A□ B□ □□□□ □□ □□□ □□ □□ □□□ □ □□□ □□□□□.

NEW QUESTION: 52

□□□ □□ □□ XSIAM□ SOAR □□□ □□□□ □□□□. □□□□□ □□ □□□ □□ □□ □□□□□ □□□□ □□□, □□□□ □□ □□□ □□□(API), □□□ □□□(ServiceNow), □ □□ HR □□□(□□ □□□)□□ □□□ □□□□□. □□ □□ □□□□ □ □□□□□ □□□ □ □□□□ □□□□ □□ □□ □□□ □□□ □□ □□□ □□□□□?

A. □□□□□□ □□□ □□□ □□□□□ □□ XSIAM □□□□ □□ □□□□□.

B. XSIAM□□ □□□□ □□□ □□ □□ □□□ □□□ □□ □□□.

C. □□ □□ □□□ API(□□□ □□□, ServiceNow, HR □□□)□ □□ □□□□ □□ □ □□ □□□□□□□.

D. XSIAM □□□□ □□□□ □□□ □□□ □□□□□(GUI) □ □□□ □ □□ □□.

E. □□□ □□□□□□ □□□ □□ PDF □□□□ □□□□ □□.

Answer: (SHOW ANSWER)

SOAR □□□□□ □□ □□□□ □□□□□ □□□□ □□□ □□□□□□ □□□□□ □□□ □□□□ □□□ □□ □□□ API□ □□ □□□ □□□ □□□□□. □□□ □□□ □□□□ □□ □ □□□□□ □□□ □□(□: □□□ □□□ □□, ServiceNow □□ □□, HR □□□ □□)□ □ □□ □ □□□□. □□ SOAR □□□□ □□□ □□ □□(A□ □□□□, B□ □□□, D□ □□□, E□ □□)□ □□□, □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□ □□□□.

NEW QUESTION: 53

□□□□ □□□ □□□□ □ □□□ XSIAM □□□□□ □□ □□ □□□ API□ □□ □□□□ □□ □□ □□□□□. □□□□□ □□ □□ '□□ API □□' □□□ □□□□□. XSIAM □□ □ □□ □□□□ □□□ □□□□ □□ □□□□ □□□ □□ □□□□ □□ □□□□ □□□ □□ □□ □□□ □□□ □□□□□ □□□□□ □□□. □□□□ □□ □□ □□ □□□□ □□ □□ □□□□ □ □□ □□□ XSIAM □□□□ □□ □□ □□ □□□ □□□□□?

A. API □□□ □□ '□□□' □□□ □□ □□□ '□□' □□□ □□ '□□' □□□ □□□□□.

B. '□□ API □□' □□□ □□ □□ □□□ □□(□□ □□□ □□)□ □□□□ '□□ □□' □□□ □□ '□□ □□'□ □□□□□.

C. □□□ □□, □□ □□□, □□ □□□ □□□ □□□□ □□□ □□ 'Python □□□□' □□□ □□□□□.

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

E. □□ □□□□□□ API □□□□ □□ □□□ XSIAM □□□ □□□ □□□□□.

Answer: (SHOW ANSWER)

□□ '□□ API □□' □□□□ □□□□ □□□ □□□□□ □□ □ □□□, □□ □□□□ □□ ('□□□□ □□ □□□'□□ □□) □□□□ □□ □□□ □□□ □□ □□□ □ □□ □□□□ □ □□ □□□□□ □□□□□ □□□ □□□ □□□□□. 'Python □□□□' □□□ □□□ □□ □ □□ □□, □□□ □□□□, □□□ □□ □□□□□ □□ □□□ □□□□ HTTP □□□ □□ □ □□□ □□□ □□□□□. 'Sleep'□ □□□□ 'Loop'□ □□□□ □□□□ □□□□□ □□ □□ □ □□ □□ □□□□ □□□ □□□□□ □□□ □ □□□□. □□ □□ □□□ □□□ □□□□ □□□ □□□□. '□□ □□'□ □□□ □□□ □□ □□□□ □□ □□□□. □□□ □□□□ □ □□ □□ □□ □□□ □□□□.

NEW QUESTION: 54

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

A. XSIAM□ □□ □□ □□□ □□(RBAC) □□□ □□□□ □□□ □□□□ □□□ □ □□ □□ □ '□□□□' □□□□□□ □□□□□.

B. □□□ □□ □□ □□□□ □□ □□□ ID □□□ □□□□□□ □□□□□ □□□□□ □□ □□ □□□□□ □□□.

C. O □□□ □□ □□ Git □□□□ □□□□ 'Production' □□□□ □□□□ □□□□□□ □□ □ □□□ □□ □□□ □□□□□.

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

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

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 □□ □□□ □□□ □□□

□ □□□□. □□ B, C, D, E□ □□□□□□□ □□□□□, XSIAM□ OT □□ □□□ □□ □□ □ □□□ □□□□ □□□ □□□□.

NEW QUESTION: 56

A. □□ A
B. □□ B
C. □□ C
D. □□ D
E. □□ E
Answer: (SHOW ANSWER)

□□ A, B, C□ □□□ □□□□□□ □□□ □□ □ □□□, '□□ □□□□ entity_id□ □□□□ □□ □□□□'□ '□□ □□□□ □□□□ □□'(□□ □□□□ □□□□ □□)□□□ □□□ □□ □□ □□□ □□□□□. □□□ □□□□, □□ □□□ □□, □□ □□ □□ □□ □□□ □□ □ □□□□ □□, □□ □□□□(□: □□ □□□□, 'for-each' □□ □□ □□□ □□ □□) □□ □□ □ □□□ □□ □□□□□□ □□ □□□ □□□ □□ □□□ □□ □□□□ □□ □ □□□□. XSIAM□ □□□□ □□□ □□ □□□□ □□□□□. □□ □□ 'entity_id'□ '□□' □□ □□ □□ □□□□ □□□ □□□ □□□ □□□ □□, □□□□□□ □□□ □□ □□□ □□ □□□□ □ □□□□ □□□□□ □□ □□□□ □□□ □□□□ □ □ □□□□. □□ □□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□□.

NEW QUESTION: 57

'□□□□□□ □□' □□□ □□ □□□ □□ 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: (SHOW ANSWER)

□ □□□ 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: 58
□□ □□ □□, □□□□ □□ □□□□ 'seclogon.exe'(RunAs) □□ 'psexec.exe'(Sysinternals)□ □□ Windows □□ □□□ □□□□ □□ □□ □□□ □□□□ □ □□□ □□□ □□□□□□. □□□ □□□ □□□□□□ □□ □□□□□. □ □□□ □□□ Process.Name□ 'seclogon.exe' □□ 'psexec.exe'□ □□ □□□ □□□□□□ □□□□ □□ □□□□ □□□□. □□ □□ □□ □□□ □□□ □□□ □□□□□ □□□□ □□□ □□□□□□ □□□ □□□ □ □□ □□□□ □. □□□ □□□ BIOC□ □□□□□ □□□□ □□□□ IT □□□□ □□□□ □□(false positive)□ □□□□ □ □□ XQL □□□ □□□□□?
A.
B.
C.
{<□>}:
D.
Answer: B (LEAVE A REPLY)
□□ B□ □□ □□□□□ □□□ XQL □□□□□. □□ A□ □□ □□□□□ □□□□ □□ □□ □□ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□□□ □□ □□□□ □□□□□. □ □ C□ psexec□ □□ □□ □□□□□□ seclogon□ □□□ □□□□. □□ D□ □□□□□□ □ □ □□□□ □□□ □□□ □□□□. □□ E□ □□ □□□□□ □□ □□□□ □□□□□. □□ B□ 'pattern' □□□ □□□□ □□ □□□□ □□□□ □□□□. □□□□ □□ □□□□ 'seclogon.exe' □□ 'psexec.exe'□ □□□ □(1□□), □□ □□□(10□ □□, □□□ □□□/□□ □□□) □□ □□ □□ □□□ □□□□□ □□□□□(2□□). 'where stage_l - Process.Reputation != 'trusted' and stage_2.Process.Reputation != 'trusted"'□ □□□ □□ □□ □□□ □□□□ □□□ □□ □□□□ □□□, □□□ □□□ □□□□ □□□ □□□□ □□ □ □□□.

NEW QUESTION: 59
Palo Alto Networks XSIAM□ □□□□ □□ □□ □□(SOC)□□ □□□□ TAXII □□□ □□ □ □□□□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□. □□□□□ □□ □□ □□ □ □ XSIAM □□□ □□□ □□□□ □□□□ □□□□ □□ □□□□□ □□□□ □□ □□□ □ □□□ □□□?
A. □□□ □□ □□ □ □□□□□ □□□ □□□□.
B. □□ □□□ □□ □□ □□ □□ □ □□ □□ □□.
C. □□, □□, □□□ □□□□ □□□ □□ □□□ □□□□.
D. TAXII □□ □□ □□□ □□ □□□ □□□ □□□□□□.
E. □□ □□□ □□ □□□ □□□ □□ □□ □□ □□□□□.
Answer: (SHOW ANSWER)
XSIAM □□□□□ □□□□ TAXII □□□ □□ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□□ □□□. □ □□ □□□□ □□□ □□ □□(TAXII □□ □□), □□(TAXII □□□□ XSIAM □□□□ □□□ □□), □□(TAXII □□□□ □□ □□ □□)□ □□ □ □ □□□□. □□□ □□□□ □□ □□□ □□□□ □□□□ □□, □□□□□ □□□ □□□ □ □ □□□□ □□□ □□ □□□□□ □□□□□. □□□□□□ □ □□□□ □□□ □□ □□ □, □□ □ □□□□ □□ □□□□□ □□□ □□ □□□ □□□□. □□□ □□□□ □□ □□ □□□ □□□ □□, □□ □□□ □□ TAXII□ □□ □□ □□ □□□□□ □□□ □□□ □□ □ □□□ □□□□ □□ □□□□.

NEW QUESTION: 60
Palo Alto Networks XSIAM□ □□□□ □□ □□ □□(SOC) □□ □□□□□ □□□ □□□ □□ □□□□ □□ 30□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□ □□□□□ □□□□ □. □□□□□ □□□□ 3 □□□□□ □□□□ □□□ □□ □□□ □□□□ □□□. □ □□ □ □□ □□ □□□ XSIAM □□□□ □□ □□□ □□□ □□□ □□□□□?
A. '□□□' □□□ □□□□ □□□□ timechart □ stdev □□□ □□□ authentication_logs□ □ □ XQL □□□□□.
B. □□□ □□ □□ □□ □□ □□□ '□□□ □□ □□' □□□□, □□□□ □□□□ □□□□ □.
C. CSV□ □□□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□ □□□□□□□□ □□ □□□.
D. □□□□□ □□ □□ □□□ □□□ □□□□ □□□ Cortex XDR □□ □□ □□□□□□□.
E. XSIAM □□□□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □□ SIEM □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
□□□ □□ □□□ □□□ □□□ □□□□□□ □□ □□ □ □□□ □□□□ XSIAM□ □□□ □□□□ □□□ □□□□□□. □□ A□ XQL(Cortex Query Language)□ □□□□ □□ □□□ □□□□□. □ □□□ □□ □□□ □□ □□□□ □□□ □ □□□, □□□□ □ (□□ □□)□ □ □ □□ □□□ □□□□ □□□□ □□□□ □□□□ □ □□□□□□. '□□□' □□□ □□□ □ □□□ □□□ stdev□ □□□□□ □ □□□□□. □□ B, C, D, E□ XSIAM□ □□□ □□□ □

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

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)□ □□□□ □□ □□ □□□□□ □□ □□□ □□ □□□□□. □□□□□ □ □□□ □ □ API □□□ □□□□ □□□ S3 □□□□ □□ □□□□ □□□□□ □□□□ □□□ □□□□ □□□ □□□ □□□□□. □□ □□□□ □□□ □□□ □□□□□.

NEW QUESTION: 62

XSIAM □□□□ □□□□□ □□ □□□ □□ □□□□□ □□□□ □□□□. □□ □□□ '□□ □ □□□□ □□ □□□□□ □□ □□□□□□ □□'□□□. XSIAM□ endpoint_status_logs□ □□ □□ □□□□□ □□ □□ is_signature_current□ □□□□ □□□□. □□□□ □□□ □□ □ □□□□ □ □□□ □□□□ □□□□ XQL □□□□ □□□□□?

A.

B.

C.

{<□>}:

D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 63

XSIAM □□□□ □□ □□ □□ □□(□: Active Directory □□□ 'username', SaaS □□□□□□ □□□ 'user_email', HR □□□ 'employee_id')□ □□□ □□□□ □□ □□□□ □□□ □□□ □ □□ □□ □□□ □□ □□□□. □□□ □□□□ □□ □□□ □□□□ □□□□□ □□□ □ □□□. □□ □□□ XQL□□ □□ □□ 'union' □ 'filter' □□□ □□□□ □□ □□ □□□ □□ □□□□. □□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□ □□□ XSIAM □□□ □ □□ □□□ □□□□ □□□?

A. □ □□ □□□ □□ '□□ □□ □□'□ □□□□ □□ □□□ □□□□ □□ □□(□: □□□ □ □□ □□)□□ □□□□□ □□ □□ □□□ □□□□ □□□ '□□□□ □□□ ID' □□□ □□□ □□.

B. □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ '□□ □□□'(□□ XSIAM '□□□ □ □□ □□')□ □□□□□. □□ □ □ □□ □□□ □ □□ □□□□ □□□□□ '□□ □□'□ □□ □□ 'canonical_user_id' □□□ □□□□□.

C. XSIAM□ '□□□ □□□' □□□ □□□□ □□□ □□□ □□□(□□□ □□, □□□, □□ ID) □ □□ 'XSIAM □□□ □□□'□ □□□□ □□□□ □□□ □□□□ □□□ □□ □□□□ □□ □□□□□ □□□□□ □□□.

D. XSIAM□ □□□□□ □□ ID □□□□□ □□□ □□□ □ □□□□ □□ □□ □□□ □□□ □□□ □□ □□□ □ □□ '□□ □□' □□□□□ □□□□.

E. □□□ □□ □□ □□□ □□□□ '□□ □□□ □□'(□: □□ □□)□ □□□□ □□□ □□□ □□ □□□□ □□ □□□ □□□ □□□□.

Answer: C (LEAVE A REPLY)

□□ □□□ □□ □□ □□□ □□□□ □□□□□ □□ □□□□ □□□□. □□ A□ B□ □□□ □□□ □□□ □□□□□, □□ C□ '□□□ □□□'□ □□□ □□□ □□ □□□ □□□ □□ □ □□□ □□□□ XSIAM □□□□□. □□□ □□□□ □□ □□□□ 'username:jsmith', 'user_email:john.smith@example.com', 'employee_id:12345'□ □□ □□□ □□□ □□□(John Smith)□ □□□□□ □□ □□□ □ □□□□. □□□ □□□□ XSIAM□ □□□ □□ □□ □□ □□ □□ □□□ □□□□□ □□□□ XQL □□□ □□□□□ □□□□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □ □□□□. □□ UBA □ □ □ □□ □□ □□□ □□□ □□□□□. □□ A□ □□□□ □□□□ □□□□ □□□/□□ □□

□ □□□ □□□. □□ 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□ E□ □□ □□□ □□□□□ □. □□ 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 □□□ □□□□ □□ □□□ □□□□□ □□ □□□□ □□□□ □□□ □□□□□. □□ □□ □□□□ □ □□□□ □□□□ □ □□□ □□ □□□ □□ □□ □□ □□ □ □□□ □□ □□□□ □□ □□□□ □□□□□ □□□□□□ □□ □□□□ □□□ □□□□ □. □□ A, C, D, E□ □□ □□□□□ □□□ □□(false positive)□ □□□□□ □□□ □□□ □ □□ □□ □ □□□□.

NEW QUESTION: 68
□ □□ □□□□ □□□ □□ □□□□□ □□□ □□□ □□□ □□ Palo Alto Networks XSIAM □ □□□□ □□□□. □□□□ □□□□ □□, □□ □□ □ □□ □□ □□□□□ □□ □□□ □□ □□□ □□□□□. □□ □□□□□□□ □□ □□ □□ □□, XSIAM □□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □ □□□□ □□ □□□□ □□□□ □□ □□□□□ □□□ □□?
A. □□ □□ □ XSIAM □□ □□□ □□ □□□□ □□ □□ □□, □□ □ □□□ □ □□□ □□ □□ TPM 2.0(□□□ □ □□ □□□ □□)□ □□ □□□□□.

B. □□□ XSIAM □□□□□ □□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□ □□□□ □□□□ □□□□(□: Intel SGX, AMD SEV).
C. □□ □□□ □□□ □□ □□ □□ □□ □□ □□□ □□□□, □□ □□□□ □□□□ □□ □□□□ □□□ □□□ □□□□□.
D. □□□□ □□□□ □□ □□□□ □□ □□□ □□ □□ □□□ '□□ □□'□, □□□ □□□ □ □□□□ □□□ □□□□□.
E. □□ □□□□ □□ □□ XSIAM □□□□ □□□ □□ □□□ □□□ □□ □□ □□□□ □□ □□(HSM)□ FIPS 140-2 □□ 3 □□ □□□ □□□□□.
Answer: A,C,D,E (LEAVE A REPLY)
□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□□. TPM 2.0(A)□ □□□□ □□ □□ □□, □□(□□□ □□□ □□), □□ □ □□□ □□□□□, □□ □ □ □ □□ □□□ □□□□□ □□□□. □□□ □□ □□ □□ □ □□(C)□ □□□ □□□ □□ □□ □□□□ □□□□□. □□ □□□ '□□ □□□(Chain of Custody)'(D)□ □□□□ □□□ □ □□□ □□ □□ □□ □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□. □□ HSM(E)□ □□□ □□□ FIPS 140-2 □□ 3 □□ □□□□□ □□□□□ □□□□ □□ □□□□ □□□□□, □□ □□ □□□ □□□ □□□ □□□□□. □□□ □□□(B)□ □□ □□□□ □□ □□□ □□ □□ □□□ □□, TPM, □□□ □□, □□□ □□, HSM□ □□ XSIAM □□□□ □ □□ '□□□ □□, □□□□ □□, □□ □□ □ □□ □□'□ □□ □□□□□ □□ □□□□ □□ □□□ □□□□□.

NEW QUESTION: 69
□□ 3□ □□□□ Cortex XSIAM□ □□□□ □□ □□□□□□□ □□□ □□□ □□□ □ □□ □□. □□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□□□, □□ □□□ □ □ □□□□□□ □□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□. □□ □□□□□□ "□ □ 3"□□□ □□□□□ □□□ □□□□, □□ □□□□□□ □□ □□□□□ □□□ □□□□ □ □ □□□□.
□□ 3□ □□□□□□ □□ □□□□ □□□□□, □□□□ □□ □□ □□□ □□□□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□□□?
A. "EG:Building3" □□□ □ □□□ □□□ □□□ Building 3□ IP □□□□ SBAC□ □□□□
B. □ □□□□ □□□ "EG:Building3" □□□ □□□ □□ □□□□ SBAC□ □□□□
C. □ □□□□ □□□ "EG:Building3" □□□ □□□ □□ □□□□ SBAC□ □□□□
D. □ □□□□ □□□ "EG:Building3" □□□ □□□□ SBAC□ □□□□□ □□□□
Answer: (SHOW ANSWER)
Building 3 □□□□□ □□ □□□ □□□□□ SBAC□ □□ □□□ □□□□□ □□□□ □□□ EG:Building3□□ □□□□ □□□. □□□ □□ □□□□ Building 3 □□ □□ □□□□□□ □ □□ □ □□□, □□ □□□□□□ □□ □□□ □□□□□ □□ □□□□□□ □□□ □□□□ □. □□, □□□□ □□ □□□ □□□ □□□□□□ □□ □□□ □□□□□.

NEW QUESTION: 70

□ □□ □□□ □□□ XSIAM□ □ □□□□□ □□□□ □□□□. □ □□□ □□ Active Directory □□□□(□□/□□□□ □□□)□ □□□□ □□□□□ ID □□□ □□□□ □□□, □ □□□ ID□ □□ Azure AD□ □□□□□. □□□ □□□ □□□ □□□□ □□ □□ □□□□ □ □ XSIAM□□ □□□ □□□ □□□□□ □□□□ □□□□. □□ □ □□□□ □□□ □□ □ □ □□□ □□□ □□ XSIAM □□□ □□□ □□□ ID □□□ □□ □□□□□ □□□ □ □□ □□ □□□ □□□□□?

A. □ □□ □□□ □□□ XSIAM □□□ VM□ □□□□, □ □□□ VM□ □□ Active Directory □□□□□ □□□□□ □□□□□. □□, □□□□ ID□ □□ □□ XSIAM Azure AD □□□□ □ □□□□.

B. Azure AD Connect□ □□□□□ □□ □□ □□□□□ Active Directory □□□□□ □□ Azure AD □□□□ □□□□□□. □□ □□, □□ □□ ID □□□□ □□□□ □□ □□□□ XSIAM Azure AD □□□□ □□□□□.

C. □□ Active Directory □□□□□ Azure AD□□ □□□ □□□□ □□□□□ □□ □□□□□ □□ □□□□ □□□ □□ □□□□□ □□□ □□, □□□ □□ XSIAM API □□□ □□□□ □ □□□□□□□□ □□□□ □□□□□.

D. □□ □□□□□ □□ □□□□ □□ Azure AD □□ □□□ □□□□□ □□□□ XSIAM□ ID □□□□□ □□□□□ Active Directory□ □□□□□ □□□□ □□□ □□□.

E. □□ □□□ □□□□□ Azure AD□□ □□ □□□ □□□□ □□ □□□□ XSIAM□ □□ □ □ □□□ □□□□ □□□ □□□□□ ID □□□ □□□□□.

Answer: B (LEAVE A REPLY)

□□□ □□□ '□□ Active Directory □□□□'□ 'Azure AD'□ '□□□ □□□ □□□□'□□□. □ □ B□ XSIAM □□□ □□□ □□□ ID□ □□□□ □□ □□□□ □□□□□. Azure AD Connect(□□ □□□ ID □□□ □□)□ □□□□□ □□ □□ □□□□□ Active Directory □□□ □□ □□ Azure AD □□□□ □□□□□ ID□ □□ '□□ □'□ □□□□□. ID □□ □□□□ □ □□ □□□ □□□□□ □□ □□□□ XSIAM Azure AD □□□□ □□□□ □□□□ ID □□□ □ □□□ □ □□□□. □ □□ □□□ ID □□□ □□ □□□□□ XSIAM□ □□□ □□□ □□ □□□, □□ □□□ □□□□ □□ □□□□□ □□□□ □□□ ID □□ □□□ □□□□□. □□ A: □□ □□□ VMS□ Azure AD □□□□ □□□□ □□□ □□□□□□, XSIAM□ □□□ ID □ □□ □□□□ XSIAM□ □□ □□ □□□ □□ □□□□ □□□ ID□ □□ □□□□ □□□ □□ □□ □□□□ □□□ □ □□□□. □□ C: ID □□□□ □□ □□□ □□ □□□□□ □□□ □□ □□ □□ □□ □□□ □□□, □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □ □□□. □□ D: □□□ □□□ □□□ □□□□□ AD □□ □□□ □□ □□□□ □□ □□□□ XSIAM □□ □□□ □□□ □□□□ □□□□ □□ □□□□□. □□ E: □□ □□□□□ ID □□ □ □□□□ □□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□□□. □□□□ □□ □ □□ □□□ □□□□ □□□ ID □□(□□, □□□, □□ □)□ □□□□□.

NEW QUESTION: 71

A. □□ A

B. □□ C

C. □□ B

D. □□ E

E. □□ D

Answer: C (LEAVE A REPLY)

NEW QUESTION: 72

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

A. □□ □□□□ □□□□ □□□ SmartScore□ □□□□□.

B. □□ □□□□ □□□□□ SmartScore□ □□□□ □□□□.

C. □□□ □□ □□□ □ SmartScore□ □□□□ □□□□.

D. □□□ □□ □□□ □ SmartScore□ □□□□□.

Answer: B (LEAVE A REPLY)

Cortex XSIAM□□ □□□ □□ □□□□ □□□□ □□□ □ □□ □□□□ □□ □□□□ □□ □□□ □□□□□ □□□ □ □□□□. □□□ SmartScore□ □□ □□□ □□□□□ □□□□ □ □□□□ □□□□.

NEW QUESTION: 73

XSIAM □□□□□ □□□□ □□□ □□ □□□□ □ □□ □□□ □□□□ □□□□. □□ XSIAM □□□□ □□□ □□□□□, □□ EU □□□ □□ □□ □□□□□ □□ □□□□ □□□ □. □□□ XSIAM □□□□ □□□ □, □□ □□ □□ □ □□□□□ XSIAM □□□□ □□ □□ □ □ □□□ □□□ □□□□ □□ □□□□ □□□ □□ □□ □□□ □□□ □□□□ □□□?

A. □□□□□ □□□□□ □□ □□□ □□□□□. □□□□□ □□□□□ □□ □□□ □□ □ □ □□□□ □□□□ □□ □□□□ □□ □□□□□.

B. □□□□ □□ □□ □□(□□) □ □□(EU) □□ URL□ □□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□□ □ □□ □□□ □□□ □□□ □ □□□ □□□.

C. XSIAM □□□□ FQDN□ □□ DNS □□ □□(□: GeoDNS)□ □□□□□. □□□□□ DNS □□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□□ □□□□.

D. □ □□□ □□ XSIAM □□□□ □□□□, □□ □□□ □□□□ □□□□□ □□□□□ □□ □□□. □□ □□□□ □□ □□ □, □□□□□ □□ □□ □□ □□□ □□ □□□□ □□ □□ □□□.

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

Answer: (SHOW ANSWER)

□□ C□ Cortex XSIAM □□□□□ □□□ □□ □□ □□□□(HA)□ □□ □□ □□□□ □□□ □ □□ □□□□□. Palo Alto Networks□ □□□ DNS □□□(Amazon Route 53 □)□ □□□□ Cortex XSIAM □□□□□ □□ □□□ □□ □□□□ □□□□ □□□□□. □□□□□ XSIAM □□□□□ FQDN(□: 'api.xdr.us.security.cortex.paloaltonetworks.com' □□ □□ □□□□ □□ □ FQDN)□ □□□ □, DNS □□ □□□□□ □□□□□ □□□□□ □□ □□□□ □□ □□□ □ □□□□ □□□□ □□□ □□□□ □ □□□□ □□□ '□□□' □□□ □□□ □□ □□ □□ □ □□□□□. □□ A□ B□ □□□ □□□□ □□□□□ □□ □□□□ □□ □□ □□□ □□□ □ □□□□□ □□□□□□. □□ D□ □□□□ □□□□ □□ □□ □□□ □□□□□ □□□□

□□□, □□□□ □□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□. □□ 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□ □□□□ □□□, □□ □□ □□(PAM) □□□ □□□□□□ □□□. □□, □□□ 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□ □□

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

NEW QUESTION: 76
XSIAM □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□□□. □□ □□ □□□□□ □ □□□ □□□□ □□, '□□□□ □□□ □□□□ □□□' □□□ □□□□□ □□□□ □□□ □ □□ □□□□ □□□□ □□□□ □□□ □□□□□. □□□□ 5□ □□□□ □□□□ □□□□ □ □□ □□□ □□ '□□□□' □□□ □□□□□ □□□. XSIAM□ □□ □□□ □□ □□□ □ □ □□ □□□□□ □□ □□□ □, □□□ □□ □□ □□□ □□□□□ □□□□ □□ □□□ □ □□ □ □□ □□□ □□□□□?
A. '□□□□ □□□ □□□□ □□' □□□ KQL □□□ □□□□ □□□□□ 5□ □□ □□ □□ □ □□□□ □□□□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
B. '□□□□ □□□ □□□□ □□' □□□ □□ XSIAM '□□'□ □□□□□. □, □ □□□ '□□' □□□□ ID□ □□ □□□ □□□□ □□□. □ □□□ XSIAM □□□ □□□□ □□ □□ □□□ □ □□ □□□□ □□□ □□ □□□□□ □□ □□□ □ XSIAM □□ □□ □□(EDL)□□ □□ □□□.
C. □□□□ □□□ □□ '□□ □□□'□ □□□ □ □□□□□ □□□□ □□□□ □□□ □□□, □□□□□ □□□ □□ □□□□□ □□□□□.
D. '□□□□ □□□ □□□□ □□' □□□ □□□□ Cortex XSOAR □□□□□ □□□□□. □ □□□ □□ □□□□□ XSIAM□ □□□□ □□ □□□□□□ □□□□, □□ □□□□□□ □□ □ 5□ □□□□ □□□□□ □□□□□ □□□□ □□□ □□□□□.
E. XSIAM□ □□ □□ □□□□□□ □□□□ □□□ □□ □□□ □□□ □□□ □□□ □□ □ □ □□□ □□□□□ □□□□ □□□□. □ □□□□□□□ □□□□□ □□ □□□□ □□ □ □□□□ □□□□□.
Answer: D,E (LEAVE A REPLY)
□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□□. □□ E□ XSIAM □ □□ □□ □□□□□□ □□ □□□ □□ □□ □□ □□ □□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□□. □ □□□□□□ □□ □□ □□□ □□ □□□ □□□ □□ □□□□ □□□ □□□□□ □□□□ □□□□. □□ D□ Cortex XSOAR□ □□□□ □□ □□ □ □□ □□□ □□□□□. □□ □□□ □□□□, □□□□(□□□□ □□)□ □□□ □□, □□ (□□/□□□□)□ □□□□□ □□□ □□□ □□□□□ □□□□ □□ □ □□□ □□□□□. □ □ A□ □□□□□□, □□ □□ □□□□□ □□ □□□□□□ □□□□ □ □□ □□□ KQL □ □□□ □□ □□ □□□□□. □□ B□ □□ □□□□ □□□□□ □□□□□, '□□' □□□ □□ □□ XSIAM□ □□□□ □□ □□□□□ □□□□□ □ □□ □□ □□ □□□ □□ XSOAR □□ □□ □ □□□□□. □□ C□ □□ □□□ □□ □□□□ □□□□□ □□ □□□ □□ □□□□ □□ □□ □□ □□ □□□ □□ □□□□ □□□□.

NEW QUESTION: 77
XSOAR(□□ Cortex XSOAR□ □□)□ □□ □□□□□□□, □□□ □ □□(SOAR) □□□□□ □□ □□□□ □□□□□ □□□□ □□□□. □ □□□□□ □□□ □□ API □□□□□□□ □ □ □□□□□ □□□□ □□□ □□□ □□ XSIAM□□ □□ □□□□□ □□□□□□□ □□□. XSOAR □□□ □□ □□□□ '□□: API □□□ □□ □□□□ □□□□□. JSON□ □□□□□ HTML□ □□□□□.'□□□. □□ □ □□ □□□ □□□□ □□□□ □ □□ □□□□ □□□ □ □□ □□□□□?
A. □□□ □□ API □□□□□□ □□ XSOAR □□ □□□ □□□□ 'Content-Type' □□□ 'application/json'□□ □□□□ □□□ □□□□□.
B. XSOAR '□□□' □□□ □□□□ □□□□ □□□ □□□□ □□□□, □□ API □□ □□□ □□□ □□□□ □□□ □□□ □□ □□□ □□□□□.
C. □□□ □□ API □□□ □□□ □□□ □□□□ XSOAR□ □□□ □□□ □□□□□, □□□ □□ □□□ □□□□ □□□□□.
D. □□□□□□ API □□ □□ □□ 'print' □□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□□□.
E. □□□□ □□□ □□□ □□ □□□□□ □□ □□□□ □□□ XSIAM □□□ □□□□□.
Answer: B,D (LEAVE A REPLY)
'□□ JSON, □□ HTML' □□ □□□□ API □□ □□□ □□□ □□ □□□ □□□□ □□□ □ □□□ □□□□□. 'Content-Type'(A)□ □□ □□(C)□ □□□□ □□ □□□ □□□ □□□□□, XSOAR□□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□□□ □□□ □□□□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□□. XSOAR □□□(B)□ □□ □□□ □□□□□ □ □□ □ □□□ □□, 'print' □□ 'log' □□□ □□□□(D) □□ □□□□ □□□□ □□□ □□□ □□□ □ □□□□. B□ D□ □□ □□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□. □□ E□ API □□ □□ □□□ □□ □□□ □□□□ □ □□ □ □□□□ □□□□□.

NEW QUESTION: 78
XSIAM □□□□ □□□□□ □□ □□□ □□ □□□□□ □□□□ □□□□. □□ □□□ '□□ □ □□□□ □□ □□□□□ □□ □□□□□□ □□'□□□. XSIAM□ endpoint_status_logs□ □□ □□ □□□□□ □□ □□ is_signature_current□ □□□□ □□□□. □□□□ □□□ □□ □ □□□□ □ □□□ □□□□ □□□□ XQL □□□□ □□□□□?
A.
B.
C.

{<□>}:
D.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
□□□ XSIAM □□□ □□□□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□ □□□□□□□. □□□□□ □□□□ □□ □□□□□. □□□□ □□□ □ □□ □□□□ API □□ □□□□ □□ □□ API □□(□: EDR□□ □□□ □□ □ □□ □□□ □□□ □□□)□ □□□ □□□□□ □□ □□□ □ □□□□. □□□□ □□ □□ □□□ □□□ □ □□□□ □□□ □□□□ □□ □□ □□ XSIAM □□□□ □□□ □□ □□□ □□□□ □□ □?
A. □□□□ □□ □□□ □□ □□ □□ □□ □□ □□ □□□ □ □□ □□ □□□□ □□□□ □.
B. □ □□ API □□ □□□ □□ □□ □□□□ □□□ '□□□ □□'□ □□□□, □□ □□□ □ □ '□□ □□' □□□ □□□□□.
C. □□ □□□ □□□□ API □□ □□□ □□□ □□□ '□□' □□□ □□□□□.
D. XSIAM □□□ □□□□ □□ □□ □□□ □□□□□□ □□ □□□ □□□□.
E. □□□ □□□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□□ □□ □□□□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
□□□□ □□□□ □□ API □□ □□ □ □□□□ □□□□□ □□ □□ API □□ □□□ □□ □□ □□□□ □□□□ '□□□ □□'□ □□□□ □□ □□□□□. □□ □□ □□□□□ □□ □ □□ □□□ □ □□□ □□□ □□□□ □□□□□ □□□□ □□□ □□□ □□□ □ □□□□. □□, □□ □□□ '□□ □□' □□ □□□□ □□ □□□□ □□□□ □□ □ □□□□□ □□□ □□□□ □□ □□□ □ □□□□. □□ A□ □□ □□□□, C□ □□□□□□, D□ □□□, E□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□□.

NEW QUESTION: 80
□ □□□ □□□□□ □□□□ □□□ □□ XSIAM □□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□□. □□ □□□ □□ □□□□□□ □□ 'Network.Protocol == 'TCP' AND Network.DestinationPort == '4444"□ □□□□□□. □ □□□ □□□ □□□□□□□□ □□ □ □□ □□□□□ □□□□□, □□□□ C2 □□□□□ □□□. □□□□ □ □□□ □□ □□□□ □□□□□□ □□□. □□ □ □ □□□□□ □□ □□□ XSIAM □□□ □□□ □□□ □□□□ □?
A. □□ 4444□ □□□□□ □□□□ □□ □□ IP □□□ □□ □□ □□□ □□□□.
B. □□ □□□ □□□□ 'LegacyAppServersGroup'□ 'Network.DestinationAddress'□ □□□□ □ □□□□.
C. □ □□ □□ □□□ □□□□. □□□ □□ 4444□ □□□□ □□□ □□□□□□□ □□ □□ □□, □□ □□□ 'Network.Protocol 'TCP' AND Network.DestinationPort '4444'□ □□ □ □□ □

□□ □□□□□. □ □□□ '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)
□□ D□ □□□□□ □□□□ □□ □□ □□□ □□□□ □ □□ □□□□□□. □□ A□ □□ □□□□□ □□(□: Word□□ □□□ □□□□ PowerShell □□□□)□□ □□□ □ □□□□.
□□ B□ □ □□□□ □□ □□ □□□□ □□ □□□ □□□□□. □□ C□ □□□□ □□□ □ □□ □□□□□ □□□ □□□□ □□□□. □□ E□ □□ □□□ □□ □□ □□□ □□□□□.
□□ D□ Word□□ □□□□ □□□ □□□□ PowerShell□ □□□□ □□□□□ □□□ □□□ □□ □□□□□□. □□ □□ □□ □□□□ □□□□□ □□□□ □ □□ □□□□ □□□□□.
□ BIOC□ □□ □□□□ □□ □□□ □□□□□□□ □□ □□□ □□□□ □□□□ □□□ □ □□ □□□.

NEW QUESTION: 83
□□ □□□□□ XSIAM□□ Cortex XDR□ □□□□□ □□□□ □□, AWS CloudTrail□ □□□ □ API □□, □□□ Okta□ ID □□ □□□ □□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □□. □ □□□ □□□ □□□□ □□ □□□ □□□□ EC2 □□□□□ □□ □□ □□□ □□□ □, □□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□.
□□□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□□ □□□□ □□ □□□ □□□□ XQL □□ □□□□ □□□□□□. □□ □□□ □□ □□□□ □□□□□ □□□ □□ □□□.
A.
B.
C.
{<□>}:
D.
Answer: D (LEAVE A REPLY)
□ □□□□□ □□□ □□□ □□□□□. □□□□ □□□ □□ □□(□□□ □□ □□□ □□), EC2□ □□ □□ □□ □□, □□□ □□□ □□('□□ □□' □ '□□□ □□'□□ □□□)□□□.
XQL □□□ □□□ □□□□ □□□ □□ □□□□ □□□□ □□□. □□ E□ □□□ □□□ □ □ □ □□□□□. 1. 'dataset = okta_authentication I filter outcome = 'SUCCESS' and authentication_method = : □□ □□□□ □□□ □□□ □□□□□ □□□□□□ □□□□ □□ □ □□□□□. □□□□□ □□□□ □□□□ □□□ □□□ □□ □□□□□. □□ □□□ □□ □□ □□ □□ □□□□ □□ □□□□ □□□□□□. 2. 'join (dataset = aws_cloudtrail I filter event_name = 'RunInstances' and event_source = 'ec2.amazonaws.com') on user_id = : □ □□ □ Okta □□ □□□□ 'RunInstances'(EC2 □□□□ □□/□□)□ □□ AWS CloudTrail □□□ □□□□□. □□ □□ □□□ □□□(Okta□ 'user_id', CloudTrail□ 'user_id')□ □□□□□. □ □□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□□□. 3. 'join (dataset = xdr_data I

filter event_type = 'Process' and process_name = 'malicious_payload.exe' and action_type = 'Process Started') on user_id = event_user and host_ip = aws_cloudtrail.source_ip_addresS : □ □□□ □□□ □□□□ □□□ □□□□□ □□□□ □□□ □□□□□□.
'malicious_payload.exe' □□□□ □□(XDR□ □□□□□ □□□)□ □□□□. □□□ □□□ □ □□□□ □□ □□(Cuser_id = event_user')□ □□□□ □□□□, □□ □□□ □□ □□□□□ □ IP □□□ CloudTrail 'RunInstanceS' □□□□ □□ IP□ □□□□ □□ □□□□□ □□ □□ □ EC2 □□□□ □□ □□ □□□ □□□ □□□□□□ □□□□□□ □□□□□. □□ □□ □ □□ □□□ □□□□□. □□ □□□□ □□□ □□□□. - A: □□□ Okta □□(□□□□ □□□ □□ □□)□ 'mfaAuthenticated=false'□ □□□□ □□ □□ □□□□□□ □□ □□□□ □□ □ □ □□□ □□ □ □□□□. - B: XDR□ □□ □□□□ □□ identity/cloud□ □□□□ □□□ □ □□ □□ □□□□□ □□□, = join □□□ □□□ □□ □□□ □□ □□□□□□. - C: src_ip_address = peer_ip_addresS□ □□□□ □□ □□□□ □□□□ □□□ □□□□□□ □ □□□ □□□□ □□ □ □□□□. □□ 'password_only'□□ □ □□□□ 'factor_type 'MFA'S'□ □□□□. - D: □□□ □□□ □□ □□ □□ □□ 'source_ip = aws_cloudtrail.source_ip_addresS' □□□ □□□□ □□□ □□□ □ □□□, 'user_id = principal_user_id'□ □□□□□□. □ □□ □□□ □□ □□□□ ID □□□□ □□□□ □□□□.

NEW QUESTION: 84
Cortex XSIAM □□□□ □□□□ □, □□ □□□□ AES 128 □□□□ □□□ □□□□□?
A. □□ -> □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□ □□□ □□□□□.
B. □□□□ "BYOK"□ □□□□ □□□ □□ □□□ □□□ □□ □□□□ □□□ □□□□.
C. AES 128□ □□□ □□ □□□□ Cortex Gateway□ □□ □□□□ □□□□□□.
D. □□□□ □□ □□□ □ □□ -> □□□ □□□□ □□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Cortex XSIAM □□□ □□□ □□ □□ □□□□ AES 128 □□□□ □□□□ □□□□□.
□□ □□□ □□ □□□□ "BYOK"(Bring Your Own Key)□ □□□□ □□□□ □□□ □□□□.
□□ □□ □□□ □ □□ □ □□□ □□ □□□ □□□□□.

NEW QUESTION: 85
□□□ □□□□ □□□ □□ □□□ □ □□ □□□ □□□□ □□□□ XSIAM □□□□□ □□ □□□□□. □ □□□□ XSOAR □□□□ □□□ □□ □□□ □□□□□□. □□ □□ □, □□ □ □□□ □□□□ □□□ □ □□□ □□□□ □□ □□ □ □□ □□ □□□□ □□ □ □□ □ □□ □□□□□ □□□ □□□?
A. □□□ □□ □□□□ □□□□ □□ □□ □□□□ □□ □□ □□ □ □□□ □□□□□. □□ □ □□□□ □□ □□□□ □□□□ □□□ □□□□□.
B. □□□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□ Docker □□□□□□ □□ □□ □ □□ □□□ □□□□□.
C. □□□□□ □□□□ □□ □□ □□(SAST) □ □□ □□(DAST)□ □□□□ □□ □□□ □□ □□□ □ □□□ □□ □□□□ □□ □□□ □□□□□.

D. XSIAM□ □□□ '□□ □□ □□' □□□ □□□□ □□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□ □□□□□ □□□□□.
E. XSOAR □□ □□□□ □□ □□□ □□ □□□□ □□ □□ □□□□ □□□□□ □□□□ □ □□□□□□ □□□□□.
Answer: A,B,C,D,E (LEAVE A REPLY)
□ □□□ □□ □□ □□□□, □□ □□□□ □□□ □ □□□ □□□□ □□ □□ □□ □□□□ □□□□ □ □□ □□□□□. -A(□□ □□/□□): □□□ □ □□ □□□ □□□ □□□□□ □□ □□□ □□□□ □ □□□ □ □□□ □□ □□ □□□ □□ □□□□ □□□□ □□ □□□□□. -B(□□□□ □□/□□ □□): XSOAR □□□ □□□□ □□□ □□□□□. □□□ □□□□□ □ □□ □□□□ □□(□: □□ □□□□□ □□ □□ □□ □□□)□ □□□ □□(CPU, □□□)□ □□□□ □□□□ □□□ □□ □□□ □□ □□ □ □□□□. -C(□□ □□/SAST/DAST): □□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□□. SAST□ □□□□ □□ □□□ □□ □ □□□, DAST(□□□□ □□ □ □□ □□)□ □□□ □□□□ □□□□ □ □□□ □. - D(□□ □□ □□): □ XSOAR □□□ □□ □□□□ □□□□ □□ □ □□□□□ □□ □□ □ □□□□□ □□□□ □□□□□ □□ □□□□ □□ □□□ □□□□□□ □□ □□□ □ □ □□□. - E(OS/□□□ □□): □□□□ □□ □□ □□ □□□□□. □□□ □ □□□ □□□□□ □ □□ OS □□ □□□□□(□: Python □□□, □□□□ □□□□□)□ □□□□ □□□□ □□ □□ □□□ □ □□□□.

NEW QUESTION: 86
□ □□□□□ 15,000□□ □□□□□, 500□□ □□□□ □□, 20□□ □□□□ □□□□ □□ □□□ □□□□ □□ Palo Alto Networks XSIAM □□□ □□□□ □□□□. □□ □□ □□ □□ □ 10TB□ □□□□, □□ □□ □□ □ □□ □□□□ □□ 20TB□ □□□□. □ □□□ □ □□ □□ □□ 90□, □ □□□□ □□ 1□ □□ □□□ □□ □□□ □□□□, □□ □□□□ 7□□ □ □□□ □□□. □ □□□□□□ □□□□ XSIAM □□□ □□ □□ □ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□ □ □□□□ □□ □□ □□ □□□ □□□ CPU □□□ □□□□□□.
B. IOPS□ □□□□ □□□ □□ □□ □□ □ □□ □□□ □□□□ □□ □ □□□ □□□□□ □□□ NVMe SSD□ □□□□□.
C. □□ □□□□□ □□□□ □ □□ □□ □□ □□□ □□ □□ GPU □□□□ □□□□□.
D. □ □□□□ □□□ □□ □□□□, □ □□□□ □□ □□□□, □□ □□□□□ □□□ □□□ □□□ □□□ □□□□□ □□□□ □□□□□ □□□□□.
E. □□□ □□ □ □□□□ □□ □□□ □□□□ □□ □□ XSIAM □□□□ □□□ 100GbE □ □□□ □□□□□□ □□□□□□□□.
Answer: (SHOW ANSWER)
□□ □□ □□□ □□ □□ □□□ □□□□ □□□ XSIAM □□ □□□□, NVMe SSD□ □□□ IOPS□ □□□□□ □□ □ □□□(B) □□□ □□□□□, □□ □ □□ □□□ □□□□ □□□ □□□□. □□ □□□□(E) □□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □ □□□ □ □□□□□. CPU □□ □□ □□□□□, □□□□ □□ □□ □□(A)□□ □ □□□ □ □□□□. XSIAM□ □□ □□□ □□ □□ CPU□ □□□□, GPU(C)□ □□□□ □□□□. □□

□□□ □□□□□ □□ □□□□□, □ □□□ 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. □□ □□
C. □□
D. □□ □□□ □□
E. □□ □□
Answer: B,C,E (LEAVE A REPLY)
□ □□□ □□□ □□□□□.A □□□ □□□: □□□ □□□□ □□ □□□ □□□□ □□ □□ □□ □□ □□□□□ □□ □□□ □□ □□□ □□□□□□ □□ □□□□ □□□□.□□ □□□ □ □□ □□□ □□□□□ □□□ '□□' □□□ □□ □□□□ □□□□□ □□□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□.B. □□ □□: □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□□.□□ □□□ □□□ □□□ □□□ □□□ □□□□□.□□□ □□ □□□ □□ □□ □ □□□ □□□□ □ □□ □□ □□□□□.C. □□: □□ □□□ □□□ '□□' □□□□ □□ □ □□□ □□□□□.□□□ □□□ □□□□□.D. □□ □□□ □□: □□□ □□□ □□ □□□ □ □□□ □□□□□ □□□□ □ □□□□□.□□ □□ □□□□ □□ □□□□□□ □□ □□□□ □□□□. E. □□ □□: □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□ □□ □□(□: □□□ □□ □□ □□, □□ □□, □□□ □ □□ □□)□ □□□ □□ □□□□□. □□ □□, '□□ IP□ trusted_ips □□□ □□ □□ □□□ □□□□'□ □□ □□□ □ □□□□. □□□ □□ □□, □□ □ □□ □□□ □□ □□□ □□ □ □□□□ □□□□□ □□□□□.

NEW QUESTION: 90
XSIAM □□□□□ □□ CMDB □□□ □□ □□□□ 'asset_criticality' □□□ □□ □□ □□□ □ □□□□ □□□□ □□ □□□ □□□ □□□□ □□□. 'High' □□□□ □□□ □□□ □□□ □□□ □□□ □□ □□□□ □□, 'Low' □□□□ □□□ □□□ □□□ □□□ □□□. 'alert.asset_criticality' □□□ 'High', 'Medium' □□ 'Low' □ □□□□ □□□ □, □□ □□□ □□ □ □□ □ □□ □□□ □□ □□ XQL □□ □□ □ □ □□□□□ □□ □ □□□□ □□ □□□ □□?
A. □□: 'alert.asset_criticality = '□□' □□: □□□ +30; □□: 'alert.asset_criticality = '□□' □□: □□□ -15. □□ □□ □□□ □□ □ □□ □□ □□ □□□□ □□□□□.
B. □□: 'alert.asset_criticality in ('High', 'Low') □□: (alert.asset_criticality = 'High') then SetTotalScore(90) else SetTotalScore(30)'.
C. □□: 'alert.asset_criticality = '□□" □□: □□ x2.0; □□: 'alert.asset_criticality = '□□' □□: □□ x0.5. □ □□ □□ □□ □□□□ □□□□□.
D. □□: 'alert.asset_criticality = '□□" □□: □□ +'alert.base_score 0.5; □□: 'alert.asset_criticality = '□□' □□: □□ '-alert.base_score 0.2.
E. □□□ XQL case □□ □□ □□ □□ □□□ □□□□□.
Answer: A,C (LEAVE A REPLY)
□□ A□ C□ XSIAM□ □□ □□□ □□□□ □□ □□□□ □□ □□□□□ □□□□ □□□□ □.□□ A(□□□ □□ □□): □□□ □□□□□ □□□ □□□□□.'□□' □□□ □□□ □□□ □□ □□□ '□□' □□□ □□□ □□□ □ □□ □□□ □□□□.□□□ □□□ □□□□□ □□ □□□□□.□□ C(□□□ □□ □□): □□ □□ □□ □□□□ □□□□□.2.0□ □□□ '□□' □

□□ □□□ □□ □□□□ 0.5□ □□□ '□□' □□□ □□□ □□□□□ □□□□ □□□□□.□ □□ □□ □□ □□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□□.□□ B(□□ □□ □ □□□ '□□ □□'): '□□ □□'□ □□□ □ □□□ XQL□□ □□ □□ □□ □□ □□□ 'if/then/else'□ □□ □□□□ □□ □□ □□□ □□ XSIAM □□ □□□ □□□ □□□□ □□ □ □□ □□□□. '□□ □□'□ □□□□□ □□□□ □□□□, □□□ □□ □□□ □□ □□□ □ □□ □□□□ □ □□ □□□ □□ □□□□□. □ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□ □□ □□□ '□□' □□ '□□'□□□ □ □□□□□ □□ □ □□□□. □□ D('base_score' □□ □□ □□): □□□□□□ □□□□□ XSIAM□ □□ □□ □□□ □□ □□□ □□ □□□ □□/□□ □ □□ '□□ □□'□ □□□□□. '□□ □□ □□' □□□□ 'alert.base_score 0.5'□ □ □ □□ □□□ □□ □□□□ □□ □□ □□ UI□ □□ □□ □□□ □□□□. □□ E('case' □□ □□ □□ □□): XSIAM□ □□ □□□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□□□ □□□□□ □□□□□. □□□ □□ □□□ '□□' □□□ □□ □□□ □□ □□□ '□□□' □□ □□ □□□□ □□(□: 'SetTotalScore' □□ □□□ 'alert.score' □□)□ UI□□ □□/□□/□□ □ □□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□□. □□□□□ □□ □□□ □□ □□ □ □□ □□□ □□□ □□□□□.

NEW QUESTION: 91
□ □□□ □□ □□ □□□ XSIAM□□ □□□□ □□□, □□ □□ □□□□□ □□□(TIP)□ □ □□□ □□ □□□ □□□□□ □□□□□ □□□. TIP□ □□ □□(IoC)□ □□ API□ □□□□ □. XSIAM □□□ □□□□ □□□□ □□ □ □□□ □□□□ □□ □□□ IOC□ □□□□□ □ □□□ □□□□ □ □□ □□□ XSIAM □□ □□ □□ □□□ □□□□□?
A. XSIAM□□ □□□ □□ BI □□□□ □□□.
B. □□ □□ □□□ □□ □□□ XSIAM □□□ □□ □□.
C. □□□ □□ □□□ □□□□ XSIAM □□ □□□□□ □□ □□□ □□□□□.
D. API□ □□ TIP□□ □□□□□ IOC□ □□□□ □□□ □□ XSOAR □□□□□ □□□□□.
E. syslog □□□□ □□ Cortex Data Lake□ IOC□ □□ □□□□□.
Answer: C (LEAVE A REPLY)
XSIAM□□ □□ TIP API□□ □□□□□ □□ □ □□ □□□ □□ □□ □□□□□ □□ □□ (C)□ □□□, XSOAR □□□□(D)□ □□ □□□□ □□□ □□□□□□. XSOAR □□□□□ □ □ □□, □□ □□, □□□ □□ □□□ □□, □□□ IOC □□□ XSIAM □□ □□□□□ □□□ □ □□□□ □□□ □ □□□ □□□□□. BI □□□□(A) □□□ □□□□ □□ □□□, □□□ □□□ □□(B) □□□ □□ □□ □□□□ □□ □□□, syslog(E) □□□ API□□ □□□□ □□ □□□□□□ □□ □□□ □□ □□□□. XSIAM□□ □□ □□□□□ □□ □□(C)□ □□□, XSOAR □□□□□ □□ API□□ □□□□ □□□□ □□ □□□ □ □□ □□□ □□□□□.

XSIAM-Engineer □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ XSIAM-Engineer □□! DumpTop □ □□ **XSIAM-Engineer** □□ □□□ □□□□□□, DumpTop XSIAM-Engineer □□ □□□ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□ □□ □□ DumpTop XSIAM-Engineer □□□ □□□□□. https://www.dumptop.com/Palo-Alto-

NEW QUESTION: 92
□□□ XSIAM □□□ □□□ □□□ □□□ □□, □□ □□□ □□ □□□ □□□□□ □□□□ □□□□. □□ □□□□ □□□□□□ □□□ □□ □□□, □□□□ □□□□ □□□□(□: OneDrive, Google Drive), □□□ □□□ □□(Microsoft 365 Exchange Online)□ □□□□□□ □ □□. □ □□ □□□ □□ □□ □□□ □□□ □□□ □□□ XSIAM□ □□□□ □□, □□ □□ □ □□□□ □□ □□□□□?
A. 1. □□□ □□(□□ □□), 2. □ □□□ □□(□□□ URL), 3. HR □□□ □□(□□ □□ □□). □□ □□□ □□□: □□ IP, □□ IP, URL.
B. 1. □□□□□ □□ □□(□□ □□□, □□□□ □□), 2. □□□□ □□□ □□ □□□(CASB) □□(□□□□ □□□□ □□□□), 3. □□□ □□□□□/M365 □□ □□(□□□ □□□, □□ □ □). □□ □□□ □□□: □□□ □□, □□ □□, □□□□ □, □□□ □□□, □□ □□ □□.
C. 1. VPN □□□ □□(□□□ □□□/□□□□), 2. Active Directory □□(□□ □□), 3. □□□□ □□ □□(□□□□□□ □□). □□ □□□ □□: □□□ ID, □□□ □□/□□, □□□□□□ □□ □□□.
D. 1. □□□□ □□ □□□(NetFlow/IPFIX), 2. □□ □□ □□□(IDS) □□, 3. □□□ □□□ □ □. □□ □□□ □□□: □□/□□ □□, □□ ID, CVE I
E. 1. □□□ □□ □□(□□□), 2. HVAC □□□ □□(□□ □□), 3. □□ □□ □□□ □□□. □ □ □□□: □□ □□, □□ □□□, □□ □□.
Answer: B (LEAVE A REPLY)
□□□ □□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□ □□ □□□□ □□ □□ □ □ □□ □□ □□□□□□ □□□ □□□□□. □□□□□ □□(□□ □□□, □□□□ □□)□ □□ □□□ □□ □□□ □□□□ □ □□ □□□□□. CASB □□□ □□□□ □□□ □□ □□□ □ □□□ □□□□ □□□ □□ □□□□ □□□□□. □□□ □□(M365 Audit)□ □□□□ □□ □ □□ □□□□ □□□□ □ □□□□□□. □□□ □□□ □□□(□□□ □□, □□ □□, □□□□ □, □□□ □□□, □□ □□ □□)□ □□□□ □□ □□ □□ □ □□□ □□□ □□□□□□.

NEW QUESTION: 93
XSIAM □□□□□ □□ □□ □□□□ □□□□□□ □□□. '□□ IP□ □□ □□ DNS □□'□ □□□□ □□□ □□□□ □□□□ □□□□□ □□ □□□□ □□□□□□ □□ □□□□□□. □□ □□□□ □□, □□□□ □□□ □□□ □□□ □□ XQL □□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□. □□ □ □□□□ □□□ □□□ □□□ □, □□ □ □□ □□□ □□□ □□□□ □□□ □□□ □□□□□ □□□□ □□□□□ □□□ XQL □□ □□□ □□□□□?
A.
B.
C.
D.

E.

Answer: (SHOW ANSWER)

□□ D□ □□□□ □□□ □□ □□□ XQL □□□□□. □□□□ □□□ □□ □□ □□□□ □ □□□□. '□□' □□□ □□(□□□□□ □□ □□□ □□□ □□ □□□□□)□□ □ □ □□ □ □□ □□□□□. □□□ □□□ 'endsWith' □□ 'contains'□ □□□□ □□ □□□□ □□ □□□ □□□ □□□□, □□ □□□□ □□□□□ □□ □ □ □□□□. □□ A□ □□ □□□ □□ □□ XDR □□□□ □□□□□. □□ B□ □□□□□ □□□□□, 'containS'□ 'endsWith'□□ □□□ □□□ □ □□□□□. □□ C□ □□□□ □□ □□ □□□ □□□ □□ □□ □□□ □□□□□ □□□□ □□□ □□ □□□□ □□ □□□ □□□□□. □□ E□ □□□□ □□□ □□ XQL □ □□ □□□ □□ □□□□□.

NEW QUESTION: 94

□□□ XSIAM □□□ VM□ □□□ □□□ □□□ □□□ □□□□□ □□□ □□ □□□ □□□ □ □□□ □□□ □□□□□□□. □□□ VM □□□ □□□□ □ VM□ XSIAM □□□□□ □□ □ □ □□ □□ XSIAM □□□ '□□□ VM □□□□'□□□ □□□□ □□□□□. □□□□ □□ □□□ □□ □□□□ □□□□□. □□□ VM □□□ □□ □□ □□ □□□ □ □□ □□□□ □ □□ TLS □□□□□ □□□ □□□□□□□. □□ □ □□ □□□ □□ □□□ □□□□, □□□ VM□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□□?

A. □□□ VM□ □□ □□(NTP)□ □□□□□ □□ □□ □□□ □□ □□□ □□□ □□□ □□ □□□. □□□ VM□□ NTP□ □□ □□□□□□.

B. □□□ VM □□□ □□□□□ □□ □□□ □□ □□□□ □□□□ □ □□□ □□□ □□ □ □□ □ □□ CA □□□□ □□□□□□□ □□□□□□□. □□□□ □□ CA □□□□ □□□ VM□ □□ □□□□ □□ □□□□ □□□.

C. □□□□ □□ □□□ VM□ □□□ □□□ □□ □□ □□□ □□□□□□□. □□□ □□□ □□□ □□□□□ □□ □□□□□.

D. □□□ VM□ □□□□ □□□□□ □□□ □□□□□ □□ □□□□□□ □□□□□□□. □ □□□ □□□ □□ □□□□□.

E. XSIAM □□□□ □ □□□□ □□□□ □□ □□□ VMS□ □□□ □□□□. Palo Alto Networks□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

□□ □□□ '□□□ □ □□ □□□□ □□□ TLS □□□□□ □□'□ '□□□ □□□ □□□ □□ □ □□□□□ □□□ □□ □□□ □□ □□□ □□'□□□. □□□ □□□□ □□□□ SSL/TLS □□□ □ □□□□□ □□□□ □□ □□□□ □□□ VM□ □□□□ □□□ □□□□. □□□ VM□ □ □□□ □□ □□□□ □□□□□ □□□□ □□ CA □□□□ □□□ VM□ □□□ □ □□ □□□ □□□□ □□□□ □□□. □□□ □□□□□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□ □ □□□□. □□ A, C, D□ □□ □□ □□□□ □□□□□ □□□□ □□□□. □□ E□ □□□□ □ □□□ □□□ VM□□ □□□ □□ □□□ VM□ □□□ □□□□.

NEW QUESTION: 95

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

□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□(□: □□□ □□ □□□ □□□□)□ □□□□ □□□ □□□□ □□□ □□ □□ □□(false positive)□ □□□□□□. □ □□□ □□□□□ □□□□□□ XSIAM □□□ XQL □□ □□□ □□ □□□ □□□□ □□□?

A. □□□ IP□ □□□□□ □□□ □□□□ '□□ □□' □□□□ 500MB□ □□□□.

B. 'network_connection' □□□ □□□ 'application_name'□ 'web-browsing' □□ 'ftp'□□ □□□ □□ □□□ □□□ □□, 'sanctioned users' □□□□ 'user_name'□ □□ □□ □□□ □□□□ □.

C. □□□□ '□□□ □□□□ □□□□ URL/IP'□ □□ □□ □□(□□□□ □□□)□ □□□□, remote_ip_addresS □□ 'url_hostname'□ □ □□ □□□ □□□ □□□□ □□□□ □□□□□ XQL□ □□□□□. □□, □□ □□□□□ □□ 'user_name' □ 'application_name'□ □□□□□ □.

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

E. XSIAM□ '□□□ □□ □□(UBA)'□ □□□□□ □□□□ □□□ □□□ □□ □□□ □□□□ □ UBA□□ □□□□ □□□ □□□□□.

Answer: (SHOW ANSWER)

□□ C□ □ □□□□□□ □□□ □□□□ □□ □□ □□□□□ □□□□ □□ □□□□□. □ □ □□ □□: □□□ □□□□ □□□□ URL/IP□ □□□□ □□□(□□ □□)□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □ □□□□□□. □□□ □□□ □□□ □□ □□□□□ □ □□□ □□□□□ □□□ □ □□□□. IP/URL □□ □□: XQL □□□ 'not in' □□ 'not (remote_ip_address in sanctioned_ips or url_hostname in sanctioned_urls)'□ □□□□ □□ □□ □□ □□□□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □ □□□□. □□□ □ □□□□ □□□ □□: 'user_name' □ 'application_name' □□□□□ □□□□ □□ □□□□ □□□ □□ □□□. □□ □□, □□ □□□ □□ □□□□□□□ □□□ □□□ □□ □□□ □□□□ □□□ □ □□□□□ □□□□ □□□□ □□ □□ □ □□□□. □□ □□ □□□ □□ □□□□ □□□ □□ □□ □□□ □ □□□□. □□ A□ □□□□ □□□□□□. □□ □□□ □□□ □□□ □□ □□ □□□ □□ □ □□□, TI □□□□ □□ □□□ □□□□ □□□□ □□ □□□□ □□□□ □. □□ B□ □□□□ □□□ □□ □□□□□□ □□□□ □□ □ □□□□. □□ D□ E□ □□ □□□, □□ □□ □□□□ □ □□□□ □□ □□□□□ □□□ □□□□□. UBA□ □□ □□□ □□□□□, □□ □□□□ IOC□ □□ □□□□ □□ □ □□□, □□ □□□ □□□□□ □□ □ □□□□.

NEW QUESTION: 96

XSIAM □□ □□ □□□□ □□□ □□ □□□ □□□□□□□. □□ □□□ □□□ Linux □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ OpenSSL□ □□ □□□□ □□□□□. □ □□□□ □□ □□□ □□□ □□□ □□□□□. XSIAM □□□□ □□□□ □□ □□□□□

□□□□ □□□ □□□□ □□, XSIAM□ '□□□' □ '□□' □□□ □ □□ □□□ □□□□□□ □□□ □□ □□□□ □ □□ □□□ □□□?

A. □□□□ □□: □□□ □□ □□ □□□□ □□ □□□ □□□□□. XSIAM □□: □□ □□ □ □□□□ □□ □□□□ □□□□ □□ OpenSSL □□□ □□□□ □□ □□□ □□□ □□□□ □. □□□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□□□.

B. □□□□ □□: □□□ □□ □□□□ □□□□□□ □□□□□. XSIAM □□: □□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□ □□□ □□ □□□□ □□□□□.

C. □□□□ □□: □□ OpenSSL □□□□ □□□□ □□ □□□□ □□ IPS □□□□□ □□□ □□. XSIAM □□: IPS□□ □□□ □□□ □□□ □□□□□ □□□ □□□ □□ □□□□ □□ □□□.

D. □□□□ □□: □□ □□□ □□ □□ □□ □□ □ □□□□□□ □□□(WAF)□ □□□□□.
XSIAM □□: WAF □□□ □□□□ □ □□□ □□□□□ OpenSSL □□□□□ □□□□ □□□ □□□□.

E. □□□□ □□: □□□ □□□□ □□ □□ □□□□ □□□□□. XSIAM□ □□: □□ □□□ □□□ □□□□□ □□ □□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

OpenSSL□ □□ □□□□ □□ □□□ □□□□ □□□□□ □□□ □□□□□. □□ □□□□ □□□ □□□ □□□□ □□□□ □□□□. XSIAM□ □□ □□ □□ □□ □□□ □□□ □□□. □□ □□ □(□□□): XSIAM □□□□□ '□□□□ □□'□□ □□□□□ □□□□□ □□□□, □□□ □□ □□□, □□□□□ □□ □□(□: 'auditd' □□, Cortex XDR□ □□ 'osquerV' □□ □), □□□□ □□ □□□□ □□□□ XSIAM□ □□□ □□□ □□□(□□□ □□ □□□□ □□ □ □□)□ □□ □□□□□ □□ □□ □□□□ □□ □□□□ □□□□ □ □□□ □ □ □□□ □. □□□□ □□(□□): □□ □□□ □□□□ □□□□□□. □□ □□ □(□□□ □ □□): XSIAM□ □□ □□□ □□□□□. □□ □□□□□ □□□ □□□□□ □□□ □□□ □□□□ □□□□ □□, XSIAM□ Cortex XDR □□□□□ □□ □□□ □□□□ □□□□□ □□□ □□ □□□ □□□ □□□□ □□ □□□□ □□□ □ □□□□(□: □□□ □□ □□□□ □□). □□ □□ □□ OpenSSL □□□ □□□ □□ XSIAM□ □□□ □□□□ □ □□□□. □□ XSIAM□ SOAR □□(□□ □□□□)□ □□□□ □□□ □□ □□□□□□ □□□□, □□□□□ □□□ □ □□□ □□□□□, □□ □□ □□□□□ □□□□□ □ □□ □□ □□ □□□ □□ □□□ □ □□□ □□□ □ □□□□. □□ XSIAM□ □□□ □□□ □□□□□□ □□□ □□ □□, □□ □ □□ □□ □□□ □□□□□ □□ □□□□□.

NEW QUESTION: 97

□□ □□□ □□ □ □□(C2) □□□ □□□ □□□□□ □□ XSIAM □□□□□ □□□□ □□ □□. □□□□□ □□□□ □□□□ □□□□. □□□□□ □□ □□□ □□□□ □□□. 1. □□ □□ IP □□□ □□□□□. 2. □□□□ □□□ □ IP□ □□ WHOIS □□□ □□□□□. 3. □□ □□ □□ □□□□□ □□□(TIPS)□□ □□ □ □□ IOC□ □□□□□. 4. □□□ □□ □□ □ □□□ □□ □□□ □□□□ □□□ □□□ □□□□□. 5. TIP□□ '□□' □□□ □□□□ API□ □□ Palo Alto Networks NGFW□□ □□ □□□□ □□□ □□ IP□ □□□□□. □□□ □□□

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

A. □□ A

B. □□ B

C. □□ C

D. □□ D

E. □□ E

Answer: C (LEAVE A REPLY)

□□ C□ □□ □□□□ □□□□ □□ □□□ □□□□□.- 'DNS □□: XSIAM □□□ □□□□ IP□ □□ □□□□□.- 'WHOIS □□□ □□' □ 'WHOIS IP □□(□□ □)': □□□ □ IP□ □□ WHOIS □□□ □□ □□ □□□□□.- 'SLOOP'('□□ API □□'□ □□ □□ TIPS□ □□): □□ □□□ □□ API□ □□□□ □□□ TIPS□ □□□□□ □□□ □ □□□□.- '□□□□ □□ □□ &'(□□□ □□□): □□□□ □□□□ □□□ □□□ □□ □□□□ □□□□ □□□ □□□□□.- '□□□□ □□ □□□□': □□□ □□ □□ □□□ □□□□□.- '□□ API □□'(NGFW API□ □ □): □□ □□ □□ □□ □□□ □□ Palo Alto Networks NGFW□ □□ □□□□ □□□□□ □ □□ □□□□□.□□ B□ □□ □□ □ □□ □□□ □ □□□□ □ □□□ '□□□ □□'□ □□□ □□.□□ A□ □□ □□□□□.□□ D□ E□ □□□□□ □□□ □□□□ □□□□□□.

NEW QUESTION: 98

□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□ XSIAM□ □□□□ □□□□. □□ □ □□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □ □□□. XSIAM□ □□□□□ □□□ □□□ □□□ □□ □ □□ □□ □□□ □□□□ □□□ □□ □□ □□ □□ □□□□□ □□□ □□□ □ □□□□?

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

B. XSIAM□ □□□ □□□□ □□□□ □□□□ □□□ □□□ □ □□□□ □□□□ □□□□ □□ □□□ □□□□□□ □□ XSIAM □□□□ □□□□□ □□□□ □□ □□□□ □□□ □□ □□□ □□□.

C. □□□ □□□ □□□□ □□ □□□□ □□□ □□□ □ □□□ □□ □□□ XSIAM □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□□□ □□□□□.

D. □□ □□ □□□ □□□□ □□ □ □□□ '□□□ □□□' □□□□ □□□ □□, □□□ □□ □□ □□□□□ □□ XSIAM □□□□□ □□□□ □□□ □□ □□□□□ □□□□□.

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

Answer: C (LEAVE A REPLY)

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

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

NEW QUESTION: 99
XSOAR □□□□□ XSIAM API □□ "Cxsiam-api-v2-get-alert-raw-data")□ □□□□ □□□ □□ □ □□ □□□ □□ □□□□ □□□□□. □ □□□ □□ ID□ □□□□ XSIAM□ □□□ □□□ □□□ 'KeyError: 'raw_data'□ □□□□ □□□ □□□□. □□ □□ □□ □□□□ □□□ □□ API □□□□ 'raw_data' □□□ □□□□ □□□ □□□ □□□□□. □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□ □ □□ □□□ □□ □□ □□□□ □□□□ □□□ □□□□□ □ □ □□□ □□□ □□□□ □□□?
A. 'xsiam-api-v2-get-alert-raw-data'□ □□□□ □□ 'wait' □□□ □□□□ □□ □□□□ XSIAM □ □□□ □□□□□□ □□□□□.
B. 'raw_data' □□ □□□□ □ □□□□ □□□□ Python '.get()' □□□□ □□□□(□: 'response.get('raw_data', OF)) □□□□ □□□□ □□ □□□ □□□□□.
C. API □□ □□ □□ □□□ 'try-except KeyError' □□□ □□□□ 'KeyError'□ □□□□ □□ □□ □□□□□ □□□□□.
D. □□□□□ □□□□□ □□ □□ □□ □□□ □□ 'raw_data'□ □□ □□□□□ XSIAM '□□ □□' □□□□ □□□□□.
E. □□□□□ 'xsiam-api-v2-get-alert-raw-data' □□□ *is-error'□ □□□□ □□(□: 'KeyError')□ □□□□ □□□□ □□□ □□ □□□□□ □□□□ '□□□' □□□ □□□□.
Answer: B,C (LEAVE A REPLY)
'KeyError'□ □□ □□□□ □□□ □□□□□. □□□(B)□ □□□□ .get()'□ □□□□ □□ 'KeyError'□ □□□□ □□ Python □□□□, □□ □□□ □□□□ □□□□□ □□ □□□ □ □ □□ □□□. □□□ □□□□ □□□ □□ □□□ □□□□ □ □□□ □□□. □□□□ 'try-except KeyError' □□(C)□ □□□□□ □□□ □□□□ □□□□ □□□□□□. □□ □□□ □ □□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □ □□□ □□ □□□□□. B□ C□ □□ □□□□ □□□ □□□□ □□□□□. □□ A□ □□□ □□ □□ □□□□ □□□□ □ □ □ □□□ □□□□ □□□ □□□□ □□□□. □□ D□ XSIAM□ □□ □□□ □□□ □□□□ □□□, □□ □□ □□□□ □□□ □□□□□ □□ □ □□□□. □□ E□ □□□ □□□ □□ □ □□ □□□□□, □□ B□ C□ □□ □□ □□□ □ □□□□ □□□ □□□□□.

NEW QUESTION: 100
XSIAM□□ '□□ □□□□ □□ □□' □□□□□ □□□□ □□□□. □□□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□□□□□ □□□ □□ □□□ □□□□□ □□ □□. □□ □□ □□□□□□ □□(□: process_events, network_connections)□ 'data_store_access_logs'□ □□□□□, □□□□□□□ □□ □□□ □□ □□ '□□' □□□ □ □□□□ □□□. □□, □□□□□□ □□□ □□□ □□□□ □□ 3□ □□□□□□□ □□ 24 □□ □□ □□□ □□ □□□ □□□□□ □□□. □□□ □□□ □□□□□ □□□ □□□□ □ □□ □□□ XSIAM XQL □□□ □□□ □□□ □□□□□?

A. □□ A
B. □□ B
C. □□ C
D. □□ D
E. □□ E
Answer: C (LEAVE A REPLY)

NEW QUESTION: 101
□□□ XSIAM □□□□□ □□ □□□□ □□□ □□□□ □□, □□ □□ 60□ □□ □□□ □□ □ □□□□□ □□□ □□□□ □□□□ □□□□ □□□. ingestion_logs □□□□□□□ □□ □□('SUCCESS', 'FAILURE', 'ERROR')□ □□□ □□ □□□ □□□□ □ □□□□ □□□ □□ □□□□ □□□□ □□□□. □□□ □□□ □□ □□□□ □□□□ □□□□ □□□. □ □□□ □□□□ □□ □□□ □□ □□□□ XQL □□□ □□□□ □□ □□□ □□□□□?
A.
B.
C.
{<□>}:
D. XSIAM□ □□□ □□□ □□□ □□□ □□ □□□ □□ □□ □□□ □□ □□□□□ □□□ □□.
Answer: (SHOW ANSWER)