Vendor: Palo Alto Networks

Exam Code: XSIAM-Engineer

Exam Name: Palo Alto Networks XSIAM Engineer

Version: DEMO

QUESTION 1
Which two requirements must be met for a Cortex XDR agent to successfully use the Broker VM as a download source for content updates? (Choose two.)

A. Device Configuration profile applied to the XDR agent must specify the Broker VM as a Download Source.
B. Agent Settings profile applied to the XDR agent must specify the Broker VM as a Download Source.
C. Broker VM must be configured with an FQDN.
D. XDR agent must authenticate to the Broker VM using a machine certificate.

Answer: BC
Explanation:
For Cortex XDR agents to use the Broker VM as a download source, the Agent Settings profile must specify the Broker VM as the update source, and the Broker VM must be configured with an FQDN so agents can reliably resolve and connect to it.

QUESTION 2
During a new Cortex XSIAM deployment, a user consistently experiences timeout sessions while trying to connect to the agent through Live Terminal, even though the firewall engineer has confirmed that all source IP addresses, port 443, and destinations are allowed.

What could be causing these persistent timeout issues?

A. User does not have administrative privileges on the managed endpoint.
B. SSL Decryption is currently being used to inspect the underlying traffic.
C. NTP is not synchronized with the server time.
D. Live Terminal feature is not supported on the current OS.

Answer: B
Explanation:
Persistent timeout issues with Cortex XSIAM Live Terminal, despite firewall rules being open, are often caused by SSL Decryption inspecting the traffic. Live Terminal relies on secure, end-to-end TLS communication, and decryption breaks this channel, leading to session failures.

QUESTION 3
Which step must be taken to enable Cloud Identity Engine on Cortex XSIAM?

A. Enable SSO integration.
B. Activate it in the Customer Support Portal.
C. Activate it on HUB.
D. Enable Active Directory log collection.

Answer: C
Explanation:
To enable Cloud Identity Engine on Cortex XSIAM, it must first be activated on HUB, Palo Alto Networks' centralized service management platform. Once activated, it can be configured and integrated with Cortex XSIAM for identity-based visibility and enforcement.

QUESTION 4
A vulnerability analyst asks a Cortex XSIAM engineer to identify assets vulnerable to newly

reported zero-day CVE affecting the "ai_app" application and versions 12.1, 12.2, 12.4, and 12.5.

Which XQL query will provide the required result?

A.
```
dataset = va_cves
| filter affected_products contains "ai_app"
| fields affected_hosts, affected_products
```

B.
```
dataset = xdr_data
| filter event_type = ENUM.PROCESS
| filter action_process_image_name = "ai_app"
| filter action_process_file_info not in ("12.1", "12.2", "12.4", "12.5")
```

C.
```
preset = host_inventory_applications
| filter application_name contains "ai_app" and version in ("12.1", "12.2", "12.4", "12.5")
```

D.
```
dataset = host_inventory
| filter applicationName contains "ai_app"
| filter applicationVersion not in ("12.1", "12.2", "12.4", "12.5")
```

Answer: C
Explanation:
The correct query is the preset = host_inventory_applications with filters for application_name contains "ai_app" and version in ("12.1", "12.2", "12.4", "12.5"). This directly identifies hosts that have the vulnerable application and specific versions installed, matching the analyst's request to find assets exposed to the zero-day CVE.

QUESTION 5
When Cortex XDR agents are on servers in a zone with no internet access, which configuration will keep them communicating with the platform?

A. Logging service in the isolated zone
B. Broker VM
C. Integration using filebeat
D. Engine

Answer: B
Explanation:
For Cortex XDR agents running on servers in zones without internet access, a Broker VM is used as a communication bridge. The Broker VM securely relays traffic between the isolated agents and the Cortex platform, maintaining connectivity without requiring direct internet access from the servers.

QUESTION 6
Which installer type should be used when upgrading a non-Linux Kubernetes cluster?

A. Standalone
B. Helm
C. Upgrade from ESM

D. Kubernetes

Answer: B
Explanation:
For upgrading a non-Linux Kubernetes cluster, the correct installer type is Helm, since Helm charts are the supported method for deploying and managing Cortex XDR agents in Kubernetes environments.

QUESTION 7
A systems engineer overseeing the integration of data from various sources through data pipelines into Cortex XSIAM notices modifications occurring during the ingestion process, and these modifications reduce the accuracy of threat detection and response. The engineer needs to assess the risks associated with the pre-ingestion data modifications and develop effective solutions for data integrity and system efficacy.

Which set of steps must be followed to meet these goals?

A. Develop an advanced monitoring system to track and log all changes made to data during ingestion, and use analytics to compare pre- and post-ingestion states based on XDM to identify and mitigate discrepancies.
B. Design a hybrid approach for critical data fields to be safeguarded against modifications during ingestion, while less critical data fields undergo allowable modifications that are rectified post-ingestion by using XDM to balance performance with data integrity.
C. Implement a pre-ingestion data validation process that aligns with the post-ingestion standards set by XDM, ensuring data consistency and integrity before it enters Cortex XSIAM.
D. Establish a process to minimize data modifications during ingestion, prioritizing raw data capture and using XDM post-

Answer: D
Explanation:
The best approach is to minimize data modifications during ingestion, prioritizing raw data capture to preserve accuracy. Then, apply XDM (XSIAM Data Model) transformations and integrity checks post-ingestion. This ensures that threat detection and response are based on unaltered, high-fidelity data while still enabling normalization and enrichment after ingestion.

QUESTION 8
A security engineer notices that in the past week ingestion has spiked significantly. Upon investigating the anomaly, it is determined that a custom application developed in-house caused the spike. The custom application is sending syslog to the Broker VM Syslog Collector applet. The engineer consults with the SOC analyst, who determines that 90% of the logs from the custom application are not used.

What can the engineer configure to reduce the ingestion?

A. Parsing rule to drop the unnecessary data at the Broker VM
B. Data model rule to drop the unnecessary data
C. Correlation rule on the Cortex XSIAM server to drop the unnecessary data
D. Data model rule to map the useful data

Answer: A
Explanation:
To reduce ingestion from the custom application, the engineer should configure a parsing rule on

the Broker VM. Parsing rules can be set to drop unnecessary data before it is ingested into Cortex XSIAM, preventing wasteful log volume and optimizing system efficiency.

QUESTION 9
An engineer is conducting a threat actor emulated test to determine which Cortex XDR module would provide protection or alert on a real-world attack. The first test was prevented.

Which action must the engineer take to enable continued testing?

A. Remove the hash from the restrictions profile.
B. Add an indicator exclusion.
C. Add a prevention rule.
D. Change the profile from "alert" to "prevent" for the BTP module.

Answer: B
Explanation:
To allow continued testing after the first emulated attack was blocked, the engineer must add an indicator exclusion. This bypasses enforcement for the specific test artifact, enabling repeated execution of the scenario to validate which Cortex XDR module detects or prevents the activity.

QUESTION 10
A Cortex XSIAM engineer adds a disable injection and prevention rule for a specific running process. After an hour, the engineer disables the rule to reinstate the security capabilities, but the capabilities are not applied.

What is the explanation for this behavior?

A. The engineer needs to restart the process to get back the security capabilities.
B. The engineer needs a support exception to get back the security capabilities.
C. The engineer needs to wait for the time period configured in the rule to pass first.
D. The engineer can disable the rule, but security capabilities are not applied to the process.

Answer: A
Explanation:
When a disable injection and prevention rule is applied to a running process, the security capabilities are detached for the lifetime of that process. Even after disabling the rule, the capabilities are not reapplied automatically; the process must be restarted to restore security enforcement.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**