Vendor: Palo Alto Networks

Exam Code: XDR-Engineer

Exam Name: Palo Alto Networks Certified XDR Engineer

Version: DEMO

QUESTION 1
Which method will drop undesired logs and reduce the amount of data being ingested?

A. [COLLECT:vendor="vendor", product="product", target_brokers="", no_hit=drop] * drop _raw_log contains "undesired logs";
B. [INGEST:vendor="vendor", product="product", target_dataset="vendor_product_raw",no_hit=drop] * filter _raw_log not contains "undesired logs";
C. [COLLECT:vendor="vendor", product="product", target_dataset="", no_hit=drop] * drop _raw_log contains "undesired logs";
D. [INGEST:vendor="vendor", product="product", target_brokers="vendor_product_raw", no_hit=keep] * filter _raw_log not contains "undesired logs";

Answer: C

QUESTION 2
Based on the image of a validated false positive alert below, which action is recommended for resolution?

A. Create an alert exclusion for OUTLOOK.EXE
B. Disable an action to the CGO Process DWWIN.EXE
C. Create an exception for the CGO DWWIN.EXE for ROP Mitigation Module
D. Create an exception for OUTLOOK.EXE for ROP Mitigation Module

Answer: D

QUESTION 3
What should be configured in Cortex XDR to integrate asset data from Microsoft Azure for better visibility and incident investigation?

A. Azure Network Watcher
B. Cloud Identity Engine
C. Cloud Inventory
D. Microsoft 365

Answer: C

QUESTION 4
What happens when the XDR Collector is uninstalled from an endpoint by using the Cortex XDR console?

A. The files are removed immediately, and the machine is deleted from the system without any retention period
B. The machine status remains active until manually removed, and the configuration data is retained for up to seven days
C. It is uninstalled during the next heartbeat communication, machine status changes to Uninstalled,

and the configuration data is retained for 90 days

D. The associated configuration data is removed from the Action Center immediately after uninstallation

Answer: C

QUESTION 5
Log events from a previously deployed Windows XDR Collector agent are no longer being observed in the console after an OS upgrade. Which aspect of the log events is the probable cause of this behavior?

A. They are greater than 5MB
B. They are in Winlogbeat format
C. They are in Filebeat format
D. They are less than 1MB

Answer: A

QUESTION 6
Which action is being taken with the query below?

```
dataset = xdr_data
| fields agent_hostname, _time, _product
| comp latest as latest_time by agent_hostname, _product | join
type=inner (dataset = endpoints
| fields endpoint_name, endpoint_status, endpoint_type) as lookup
lookup.endpoint_name = agent_hostname
| filter endpoint_status = ENUM.CONNECTED
| fields agent_hostname, endpoint_status, latest_time, _product
```

A. Monitoring the latest activity of endpoints
B. Identifying endpoints that have disconnected from the network
C. Monitoring the latest activity of connected firewall endpoints
D. Checking for endpoints with outdated agent versions

Answer: A

QUESTION 7
Based on the SBAC scenario image below, when the tenant is switched to permissive mode, which endpoint(s) data will be accessible?

A. E1 only

B. E2 only
C. E1, E2, and E3
D. E1, E2, E3, and E4

Answer: C

QUESTION 8
An analyst considers an alert with the category of lateral movement to be allowed and not needing to be checked in the future. Based on the image below, which action can an engineer take to address the requirement?

A. Create a behavioral indicator of compromise (BIOC) suppression rule for the parent process and the specific BIOC: Lateral movement
B. Create an alert exclusion rule by using the alert source and alert name
C. Create a disable injection and prevention rule for the parent process indicated in the alert
D. Create an exception rule for the parent process and the exact command indicated in the alert

Answer: B

QUESTION 9
Some company employees are able to print documents when working from home, but not on network-attached printers, while others are able to print only to file. What can be inferred about the affected users' inability to print?

A. They may be attached to the default extensions policy and profile
B. They may have a host firewall profile set to block activity to all network-attached printers
C. They may have different disk encryption profiles that are not allowing print jobs on encrypted files
D. They may be on different device extensions profiles set to block different print jobs

Answer: B

QUESTION 10
Which two steps should be considered when configuring the Cortex XDR agent for a sensitive and highly regulated environment? (Choose two.)

A. Enable critical environment versions
B. Create an agent settings profile where the agent upgrade scope is maintenance releases only
C. Create an agent settings profile, enable content auto-update, and include a delay of four days
D. Enable minor content version updates

Answer: BC

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**