DUMPSARENA

Palo Alto Networks XSIAM Analyst

Palo Alto Networks XSIAM-Analyst

Version Demo

Total Demo Questions: 7

Total Premium Questions: 70

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, XSIAM Architecture	7
Topic 2, Data Integration	3
Topic 3, Detection Engineering	12
Topic 4, Incident Investigation	25
Topic 5, Threat Hunting	11
Topic 6, Automation	12
Total	70

QUESTION NO: 1

An analyst is creating an indicator prevention rule for a newly identified threat campaign. The rule must prevent selected malicious indicators only on endpoint groups that use designated prevention profiles.

Which two configuration steps are required before the analyst reviews and saves the rule? (Choose two.)

A. Filter and select one or more supported file, IP address, or domain indicators.

B. Select the prevention profiles to which the rule will apply.

C. Set the indicator prevention rule severity to Critical.

D. Create an alert exclusion for the selected indicators.

ANSWER: A B

Explanation:

The analyst must select one or more supported indicators that should trigger prevention and select the prevention profiles that enforce the rule. These steps define both what is prevented and where the prevention rule applies.

Indicator prevention rules are not configured by selecting arbitrary indicator types or by setting an alert severity. An alert exclusion suppresses alert generation and is not a mechanism for applying endpoint prevention to selected indicators.

QUESTION NO: 2

A playbook developer creates a reusable workflow that accepts an indicator as input, enriches it, and returns a verdict to the calling playbook. The same workflow must be invoked by phishing, malware, and network investigation playbooks.

Which playbook task type is most appropriate for invoking the reusable workflow?

A. Sub-playbook

B. Standard

C. Conditional

D. Manual

ANSWER: A

Explanation:

A Sub-playbook task is designed to invoke reusable playbook logic from a parent playbook. It can receive inputs from the calling workflow and return outputs that the parent workflow can use for subsequent decisions or response actions.

A Standard task runs an individual command or automation, while a Conditional task selects a branch. Recreating the entire workflow separately in each incident playbook would reduce consistency and make maintenance more difficult.

QUESTION NO: 3

SCENARIO:

A security analyst has been assigned a ticket from the help desk stating that users are experiencing errors when attempting to open files on a specific network share. These errors state that the file format cannot be opened. IT has verified that the file server is online and functioning, but that all files have unusual extensions attached to them.

The security analyst reviews alerts within Cortex XSIAM and identifies malicious activity related to a possible ransomware attack on the file server. This incident is then escalated to the incident response team for further investigation.

Upon reviewing the incident, the responders confirm that ransomware was successfully executed on the file server. Other details of the attack are noted below:

• An unpatched vulnerability on an externally facing web server was exploited for initial access

• The attackers successfully used Mimikatz to dump sensitive credentials that were used for privilege escalation

• PowerShell was used on a Windows server for additional discovery, as well as lateral movement to other systems

• The attackers executed SystemBC RAT on multiple systems to maintain remote access

• Ransomware payload was downloaded on the file server via an external site "file io"

QUESTION STATEMENT:

The incident responders are attempting to determine why Mimikatz was able to successfully run during the attack.

Which exploit protection profile in Cortex XSIAM should be reviewed to ensure it is configured with an Action Mode of Block?

A. Logical Exploits Protection

B. Browser Exploits Protection

C. Known Vulnerable Process Protection

D. Operating System Exploit Protection

ANSWER: C

Explanation:

Known Vulnerable Process Protection is the appropriate profile to review because it is designed to protect processes that are commonly targeted or abused during endpoint attacks. In this scenario, Mimikatz was used to dump credentials, a high-impact credential-access technique that can enable privilege escalation and subsequent lateral movement. Reviewing this protection profile confirms that the relevant protection rule is enabled and that its Action Mode is set to **Block**, rather than report-only or another non-preventive behavior. A Block action is important because it instructs the Cortex XSIAM agent to prevent the protected malicious or exploit-related activity on the endpoint, reducing the opportunity for attackers to obtain reusable credentials and advance the intrusion. Profile configuration must also be assigned through the applicable endpoint security policy and deployed to the affected Windows server; merely creating or editing a profile does not protect an endpoint until policy enforcement is in place. Palo Alto Networks documents the configuration and assignment of exploit protection profiles in its Cortex XDR endpoint-security guidance, which underpins Cortex XSIAM endpoint prevention capabilities. See Manage Exploit Protection Profiles and Cortex XDR Endpoint Security.

QUESTION NO: 4

An analyst confirms that a ransomware process is actively encrypting files on a workstation and that the endpoint is making connections to additional internal systems.

Which two Cortex XSIAM response actions provide the most immediate containment? (Choose two.)

A. Terminate the ransomware process.

B. Isolate the endpoint.

C. Run an on-demand malware scan.

D. Remove a detected malicious file.

ANSWER: A B

Explanation:

Terminating the malicious process stops the currently observed encryption activity on the endpoint. Isolating the endpoint restricts its network communications, reducing the opportunity for ransomware operators or malware to reach other internal systems, communicate with command-and-control infrastructure, or continue lateral movement.

Removing a malicious file can be appropriate remediation when the relevant artifact is identified, but it does not necessarily stop an already running process. A malware scan assists with detection and remediation but is not the immediate containment action required by the scenario.

QUESTION NO: 5

Which query will hunt for only incoming traffic from 99.99.99.99 when all log sources have been mapped to XDM?

A. datamodel preset = * | filter XDM.ALIAS.ip = "99.99.99.99"

B. datamodel dataset = * filter XDM.ALIAS.ipv4 = "99.99.99.99"

C. datamodel dataset = * | fields fieldset.xdm_network | filter xdm.source.ipv4 = "99.99.99.99"

D. preset = network_story | filter agent_ip_addresses = "99.99.99.99"

ANSWER: C

Explanation:

`datamodel dataset = * | fields fieldset.xdm_network | filter xdm.source.ipv4 = "99.99.99.99"` is the appropriate XQL query because it searches across all datasets that have been normalized into the Cortex XSIAM Data Model, then applies the standard network field set before filtering on the normalized source IPv4 field. In XDM, `xdm.source.ipv4` represents the source-side IPv4 address associated with a network event. Filtering that field for `99.99.99.99` therefore identifies events in which that address is the traffic origin, which is the intended meaning of incoming traffic from the specified external IP. The `fields fieldset.xdm_network` stage is important because it scopes the query to normalized network-oriented fields and supports a consistent hunt even when the underlying telemetry originates from different products or vendors. Using `datamodel dataset = *` allows the hunt to cover all available XDM-mapped datasets rather than requiring knowledge of an individual raw-log dataset. This approach relies on the common XDM schema, enabling the same query to work across mapped log sources. Palo Alto Networks documents XQL pipeline syntax and commands in the XQL Language Reference; XDM normalization concepts are covered in the Cortex Data Model documentation.

QUESTION NO: 6

In which two locations can mapping be configured for indicators? (Choose two.)

A. Feed Integration settings

B. Classification & Mapping tab

C. STIX parser code

D. Indicator Configuration in Object Setup

ANSWER: A B

Explanation:

Feed Integration settings and the **Classification & Mapping tab** are the two locations used to configure indicator mapping in Cortex XSIAM. When configuring a threat-intelligence feed, Feed Integration settings provide the feed-specific configuration needed to ingest indicator data and associate incoming values with the appropriate indicator attributes. This is useful when a particular source has its own field names or data layout that must be normalized as it is brought into the platform.

The Classification & Mapping tab provides the mapping workflow for defining how incoming data is classified and how source fields populate Cortex XSIAM fields. For indicators, this lets an analyst ensure that values such as the indicator type, value, reputation, expiration, tags, and other contextual fields are interpreted consistently. Using both locations supports reliable ingestion and normalization of external intelligence, so indicators are usable for searches, enrichment, correlation, and investigations. Palo Alto Networks describes indicator management and threat-intelligence ingestion in its Indicators documentation and documents the platform's ingestion and mapping concepts in the Integrations documentation.

QUESTION NO: 7

An analyst is responding to a critical incident involving a potential ransomware attack. The analyst immediately initiates full isolation on the compromised endpoint using Cortex XSIAM to prevent the malware from spreading across the network. However, the analyst now needs to collect additional forensic evidence from the isolated machine, including memory dumps and disk images without reconnecting it to the network. Which action will allow the analyst to collect the required forensic evidence while ensuring the endpoint remains fully isolated?

A. Using the endpoint isolation feature to create a secure tunnel for evidence collection

B. Collecting the evidence manually through the agent by accessing the machine directly and running "Generate Support File"

C. Using the management console to remotely run a predefined forensic playbook on the associated alert

D. Disabling full isolation temporarily to allow forensic tools to communicate with the endpoint

E. Physically access the endpoint and use approved local forensic tools to capture memory and create a disk image on controlled removable media.

ANSWER: E

Explanation:

Use approved local forensic acquisition tools while physically accessing the endpoint, and save the resulting memory dump and disk image to controlled removable media. This approach preserves full network isolation because acquisition occurs directly on the host and does not require the host to communicate with Cortex XSIAM, a management service, or another network-connected forensic system. The analyst can use an organization-approved incident-response workflow to attach trusted, write-protected or otherwise controlled storage, capture volatile memory before shutdown or imaging activity, then acquire the required disk evidence and maintain chain-of-custody records for the collected media.

This is appropriate for the stated evidence types. Memory capture requires a tool running on the affected endpoint, and a forensic disk image is normally written to locally attached storage or collected through an offline process. Cortex XSIAM endpoint isolation is intended to contain a potentially compromised device by restricting its network communications; retaining that containment state while performing a hands-on acquisition avoids reopening a potential ransomware propagation path. Palo Alto Networks documents endpoint isolation behavior and the administrative isolation workflow in its endpoint isolation documentation. For handling and preserving acquired digital evidence, see the NIST guide to forensic techniques in incident response.