DUMPSARENA

Palo Alto Networks XSIAM Engineer

Palo Alto Networks XSIAM-Engineer

Version Demo

Total Demo Questions: 8

Total Premium Questions: 81

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Components	4
Topic 2, Data Collection and Integration	22
Topic 3, Detection and Analysis	9
Topic 4, Investigation and Response	3
Topic 5, Automation and Orchestration	15
Topic 6, Administration and Maintenance	28
Total	81

QUESTION NO: 1 - (SIMULATION)

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: See the explanation for the answer

Explanation:

Correct answer: B. Add an indicator exclusion.

Because the emulated threat was prevented on the first run, add an **indicator exclusion** for the relevant test indicator (for example, its file hash). This permits the known test artifact to execute so testing can continue and the engineer can identify the Cortex XDR module that generates alerts or protection for the attack behavior.

Removing a hash from a restrictions profile or changing a module from alert to prevent does not provide the required targeted allowance for the test artifact. A prevention rule would further block activity rather than enable it.

QUESTION NO: 2

When activating the Cortex XSIAM tenant, how is the data at rest configured with AES 128 encryption?

A. Under Advanced - > Encryption Method, choose the desired encryption method during the initial setup of the tenant.

B. Under Advanced, choose " BYOK, " and adhere to the wizard ' s instructions as outlined in the encryption method section.

C. Create encryption keys with AES 128 and upload it securely through Cortex Gateway.

D. Under Advanced - > Encryption Method, choose the desired encryption method after the initial setup of the tenant.

ANSWER: A

Explanation:

Under Advanced - > Encryption Method, choose the desired encryption method during the initial setup of the tenant. Encryption settings are selected as part of the Cortex XSIAM tenant activation workflow, before the tenant is fully provisioned. The Advanced settings area exposes the available encryption-method choices, allowing the administrator to select the organization’s required data-at-rest encryption configuration at the appropriate point in deployment. Cortex XSIAM protects stored tenant data through encryption at rest, and selecting the encryption method during activation ensures that the tenant is provisioned with the intended key-management and encryption arrangement from the outset. This is important because encryption is a foundational tenant-level setting rather than an operational configuration normally deferred until after initial setup. Palo Alto Networks documents tenant activation and its available advanced configuration settings in the Cortex XSIAM Administrator’s Guide. For broader platform documentation and administrative guidance, consult the Cortex XSIAM Administrator’s Guide and the Cortex XSIAM product overview.

QUESTION NO: 3

Based on the images below, which command will allow the context data to be displayed as a table when troubleshooting a playbook task?

A. !ConvertTableToHTML table=${parentIncidentFields.custom_fields}

B. !JsonToTable value=${parentIncidentFields.custom_fields}

C. !ToTable data=${parentIncidentFields.custom_fields.incidentassignment}

D. !ExtractHTMLTables html=${parentIncidentFields.custom_fields.incidentassignment}

ANSWER: C

Explanation:

`!ToTable data=${parentIncidentFields.custom_fields.incidentassignment}` is the correct command because the `ToTable` automation takes data from the specified Cortex XSOAR context path and renders it as a human-readable table in the War Room. The context expression targets the `incidentassignment` value under the parent incident's custom fields, rather than passing the entire custom-fields object. This is useful during playbook troubleshooting because nested context values can otherwise be difficult to inspect in their raw JSON-like representation. Running the command makes the individual properties in the assignment data—such as status, dates, and related values—visible as structured table columns and rows, allowing an analyst to validate what a task received or produced. Cortex XSOAR commands use the `!` prefix, and context values are supplied through the `${...}` context-expression syntax. The command can be run in the War Room while investigating the execution state of a playbook task, without changing the underlying incident context. Palo Alto Networks documents the ToTable automation and its `data` argument in the ToTable script reference; see also the Cortex XSOAR context documentation for context-path usage.

QUESTION NO: 4

Before running a malware scan on a Linux endpoint, an engineer notices that the Cortex XDR agent operational status is **Partially Protected**. No recent prevention-policy changes have been made in Cortex XSIAM.

Which two conditions can explain this status? (Choose two.)

A. The endpoint has reached its configured malware-scan limit.

B. The Linux kernel modules required by the agent failed to load.

C. The installed Cortex XDR agent version is not compatible with the endpoint operating system or kernel.

D. The endpoint has been excluded from an alert notification rule.

ANSWER: B C

Explanation:

A Linux agent can report as partially protected when required kernel modules fail to load, including when the installed kernel is unsupported. An outdated agent can also lack compatibility with the current Linux distribution or kernel and should be evaluated against the supported-agent and operating-system compatibility requirements. A server-side policy change is not required for either endpoint-specific condition.

QUESTION NO: 5

A Cortex XSIAM engineer is implementing role-based access control (RBAC) and scope-based access control (SBAC) for users accessing the Cortex XSIAM tenant with the following requirements:

Users managing machines in Europe should be able to manage and control all endpoints and installations, create profiles and policies, view alerts, and initiate Live Terminal, but only for endpoints in the Europe region.

Users managing machines in Europe should not be able to create, modify, or delete new or existing user roles.

The Europe region endpoints are identified by both of the following:

Endpoint Tag = "Europe-Servers" and Endpoint Group = "Europe" for servers in Europe

Endpoint Group = "Europe" and Endpoint Tag = "Europe-Workstation" for workstations in Europe

Which two sets of implementation actions should the engineer take? (Choose two.)

A. Verify and confirm that SBAC mode under "Server Settings" is set to "Restrictive," and assign "EG:Europe" under the user permission scope configuration.

B. Use the pre-defined roles, assign the "Instance Administrator" role to the user or user group managing Europe-based endpoints.

C. Verify and confirm that SBAC mode under "Server Settings" is set to "Permissive," and assign "EG:Europe" under the user permission scope configuration.

D. Use the pre-defined roles, assign the "Privileged IT Admin" role to the user or user group managing Europe-based endpoints.

ANSWER: A D

Explanation:

Scope-based access control must be enabled in **Restrictive** mode and the **EG:Europe** endpoint-group scope must be assigned to the relevant users or user group. Restrictive mode ensures that permissions granted through the role are applied only to entities included in the assigned scope. Because both the Europe servers and Europe workstations belong to the Europe endpoint group, using **EG:Europe** covers both device populations without having to create separate scopes based on their distinct endpoint tags. This enforces the regional boundary while allowing the team to perform their endpoint-management duties within that boundary.

The **Privileged IT Admin** predefined role supplies the operational endpoint permissions required for this scenario, including endpoint and agent management, profile and policy administration, alert visibility, and Live Terminal access. It is appropriate for an IT operations team that needs broad device-administration capabilities but must not administer tenant user roles. Combining this RBAC role with the Europe endpoint-group scope implements least-privilege access: the role determines what administrative actions the users can perform, and the scope determines which Europe endpoints those actions can affect. Palo Alto Networks describes these access-control concepts in its Cortex XSIAM access-management documentation and SBAC configuration guidance.

QUESTION NO: 6

What is the primary function of the URL " -docker.pkg.dev" in the context of a Palo Alto Networks infrastructure?

A. It downloads Docker content updates.

B. It downloads Kubernetes images for agent installation.

C. It imports Docker licensing.

D. It downloads Engine Docker containers.

ANSWER: D

Explanation:

The URL pattern `<region>-docker.pkg.dev` is a regional Google Artifact Registry hostname used to retrieve container images. In a Cortex XSIAM deployment, the Engine requires its Docker container images to be available locally so that its services can be deployed and run. Therefore, “It downloads Engine Docker containers.” is correct: the Engine host connects to the appropriate regional registry endpoint and pulls the required Engine images. The `<region>` portion identifies the Google Cloud region hosting the registry, which allows the deployment to retrieve the intended image artifacts from the correct regional repository. Google documents that Artifact Registry uses repository URLs in the form `LOCATION-docker.pkg.dev/PROJECT-ID/REPOSITORY/IMAGE` for Docker images, directly matching this hostname pattern. In practical XSIAM Engine network planning, outbound access to the applicable registry endpoint is needed during image retrieval and updates, alongside the other documented Engine connectivity requirements. See the Google Artifact Registry Docker documentation and the Cortex XSIAM documentation.

QUESTION NO: 7

An engineer attaches an alert context as test data while debugging a playbook. The playbook contains one task that updates a list and another task that writes values into incident context.

Which two statements are correct for this debugging session? (Choose two.)

A. Changes to the test incident context do not alter the original alert context.

B. Changes made by a list-update task alter the original list object.

C. Debug mode automatically prevents all external and shared-object changes.

D. Updating incident context in the debugger updates the source alert context immediately.

ANSWER: A B

Explanation:

Attached alert context is used as test data, so changes made to incident context during the debugger session do not alter the original alert context. Lists are shared tenant objects, however. A task that adds or removes list entries during debugging changes the actual list.

Engineers should use dedicated test lists or avoid write operations when debugging playbooks that interact with operational allowlists, blocklists, or other shared list objects.

QUESTION NO: 8

A Behavioral Threat Protection (BTP) alert is triggered with an action of "Prevented (Blocked)" on one of several application servers running Windows Server 2022. The investigation determines the involved processes to be legitimate core OS binaries, and the description from the triggered BTP rule is an acceptable risk for the company to allow the same activity in the future.

This type of activity is only expected on the endpoints that are members of the endpoint group "AppServers," which already has a separate prevention policy rule with an exceptions profile named "Exceptions-AppServers" and a malware profile named "Malware-AppServers."

The CGO that was terminated has the following properties:

SHA256: eb71ea69dd19f728ab9240565e8c7efb59821e19e3788e289301e1e74940c208

File path: C:\Windows\System32\cmd.exe

Digital Signer: Microsoft Corporation

How should the exception be created so that it is scoped as narrowly as possible to minimize the security gap?

A. Create the exception via the alert itself, selecting the CGO hash, CGO signer, CGO process path, and applying the scope to the "Exceptions-AppServers" profile.

B. Create a Disable Prevention Rule via Exceptions Configuration with the following selections:

C. Create a Legacy Agent Exception via Exceptions Configuration with the following selections:

D. Create the exception via the alert itself, selecting the CGO hash, CGO signer, CGO process path, and applying the scope to "Global."

ANSWER: B

Explanation:

Create a Disable Prevention Rule through Exceptions Configuration and assign it to the *Exceptions-AppServers* exceptions profile. The exception should target the triggered Behavioral Threat Protection prevention rule while using the identified causality group owner attributes: the stated SHA256 value, the Microsoft Corporation signer, and `C:\Windows\System32\cmd.exe` path. Combining these attributes provides a highly specific identity for the permitted executable, rather than allowing a broad category of behavior. Scoping the exception to the existing AppServers-specific exceptions profile ensures that only endpoints receiving that prevention policy can use the exception. This follows the least-privilege approach: the accepted BTP activity remains permitted only where it is expected and only for the verified Windows binary involved in the investigated alert. Palo Alto Networks documents exception management and the use of exception profiles to apply endpoint-specific exclusions in its Configure Exceptions documentation. Additional context on Behavioral Threat Protection and prevention-rule handling is available in the Behavioral Threat Protection documentation.