ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

How will Cortex XSIAM help with raw log ingestion from third-party sources in an existing infrastructure?

A. Any structured logs coming into it are left completely unchanged, and only metadata is added to the raw data.

B. For structured logs, like CEF, LEEF, and JSON, it decouples the key-value pairs and saves them in table format.

C. Any unstructured logs coming into it are left completely unchanged, and metadata is not added to the raw data.

D. For unstructured logs, it decouples the key-value pairs and saves them in a table format.

Answer: B

Explanation:

Cortex XSIAM ingests structured third-party logs (such as CEF, LEEF, and JSON) by breaking down the key-value pairs and saving them in a normalized table format. This enables efficient correlation, analytics, and query performance across diverse log sources while preserving data fidelity.

Question: 2

In which two locations can correlation rules be monitored for errors? (Choose two.)

A. XDR Collector audit logs (type = Rules, subtype = Error)

B. correlations_auditing dataset through XQL

C. Management audit logs (type = Rules, subtype = Error)

D. Alerts table as a health alert

Answer: A, B

Explanation:

Correlation rule errors can be tracked in XDR Collector audit logs (type = Rules, subtype = Error) and by querying the correlations_auditing dataset through XQL. These provide visibility into execution issues and failures for correlation rules.

Question: 3

Which option should be used when customizing a dashboard in Cortex XSIAM to include a widget that will display data filtered by more than one dynamic value?

A. Free text/number

B. Multi-select

C. Fixed filter

D. Single-select

Answer: B

Explanation:

The Multi-select option allows a dashboard widget in Cortex XSIAM to be filtered by more than one dynamic value, enabling flexible data exploration and visualization across multiple selected criteria.

Question: 4

How must Cloud Identity Engine be deployed and activated on Cortex XSIAM?

A. In a different region than Cortex XSIAM; logs can be verified using pan_dss_raw dataset

B. In a different region than Cortex XSIAM; logs can be verified using endpoints dataset

C. In the same region as Cortex XSIAM; logs can be verified using pan_dss_raw dataset

D. In the same region as Cortex XSIAM; logs can be verified using endpoints dataset

Answer: C

Explanation:

Cloud Identity Engine must be deployed in the same region as Cortex XSIAM to ensure compliance and proper data handling. Once integrated, the ingestion can be verified by checking the pan_dss_raw dataset, which records the raw directory synchronization logs.

Question: 5

Which common issue can result in sudden data ingestion loss for a data source that was previously successful?

A. Data source is using an unsupported data format.

B. Data source has reached its maximum storage capacity.

C. Data source has reached its end of life for support.

D. API key used for the integration has expired.

Answer: D

Explanation:

A sudden data ingestion loss for a previously successful data source commonly occurs when the API key used for the integration has expired, breaking authentication and preventing further log collection.

Question: 6

While using the remote repository on a Development XSIAM tenant, which two objects can be pushed or pulled to the remote repository? (Choose two.)

A. Scripts

B. Parsing rules

C. iLists

D. Layouts

Answer: A, C

Explanation:

When working with a remote repository on a Development XSIAM tenant, Scripts and Lists can be pushed or pulled. These objects are version-controlled and portable across environments for

development and deployment.

Question: 7

When a Cortex XSIAM playbook execution reaches a breakpoint on a non-manual task, which two actions will allow the playbook to continue? (Choose two.)

A. Disable the breakpoint and rerun the playbook from the start.

B. Skip the task with the breakpoint to let the playbook proceed automatically.

C. Wait for all parallel tasks to be completed before the breakpoint task resumes automatically.

D. Click Run Script Now or Complete Manually.

Answer: B, D

Explanation:

When a playbook execution reaches a breakpoint on a non-manual task, you can skip the task with the breakpoint to allow the playbook to continue, or manually trigger continuation using "Run Script Now" or "Complete Manually". These actions resume execution without restarting the entire playbook.

Question: 8

What is the purpose of using rolling tokens to manage Cortex XDR agents?

A. To periodically rotate encryption keys used for tenant communication

B. To perform administration on agents without requiring static credentials

C. To authorize agents to download and install content updates

D To temporarily disable the agents during maintenance windows

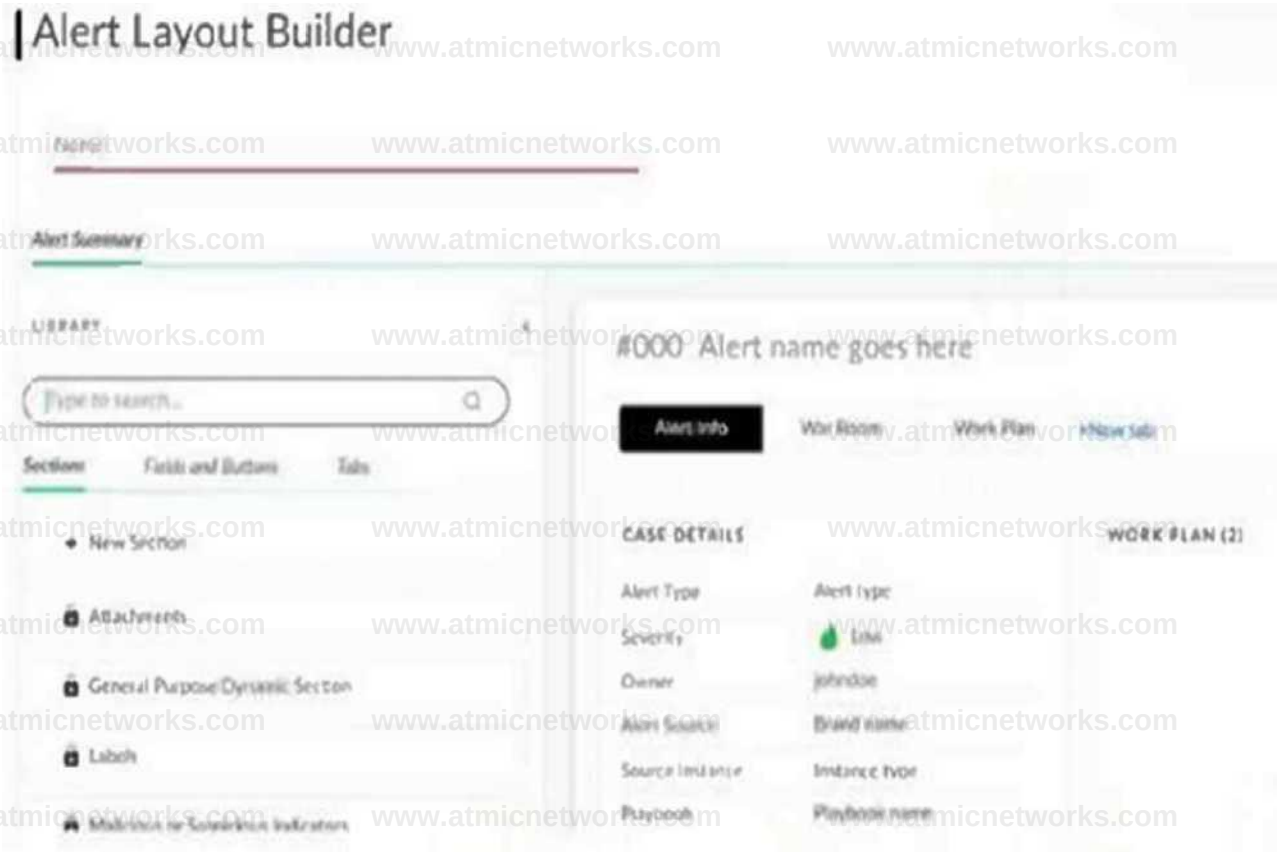
Answer: B

Explanation:

Rolling tokens in Cortex XDR are used to perform administration on agents without relying on static credentials. This improves security by providing time-limited, automatically rotating tokens that maintain agent management access without exposing long-lived credentials.

Question: 9

Based on the image below, which statement applies to the ability to remove tabs when creating a new alert layout?



A. Only "Alert Info" tab can be removed.

B. Only "Alert Info" and "War Room" tabs can be removed.

C. Only "War Room" and "Work Plan" tabs can be removed.

D. Only "Work Plan" tab can be removed.

Answer: C

Explanation:

In Cortex XSIAM's Alert Layout Builder, the "War Room" and "Work Plan" tabs are optional and can be removed, while the "Alert Info" tab is mandatory and cannot be deleted. This ensures that essential alert details are always retained, while collaboration and workflow tabs can be customized.

Question: 10

A Cortex XSIAM engineer is developing a playbook that uses reputation commands such as '!ip' to enrich and analyze indicators.

Which statement applies to the use of reputation commands in this scenario?

A. If no reputation integration instance is configured, the '!ip' command will execute but will return no results.

B. Reputation commands such as '!ip' will fail if the required reputation integration instance is not configured and enabled.

C. The mapping flow for enrichment commands is disabled if extraction is set to "None."

D. Enrichment data will not be saved to the indicator unless the extraction setting is manually configured in the playbook task.

Answer: B

Explanation:

Reputation commands such as !ip rely on a configured and enabled reputation integration instance (for example, VirusTotal, Palo Alto WildFire, or other threat intel sources). If no such instance is available, the command execution will fail, since it cannot retrieve enrichment data.

Question: 11

An engineer wants to onboard data from a third-party vendor's firewall. There is no content pack available for it, so the engineer creates custom data source integration and parsing rules to generate a dataset with the firewall data.

How can the analytics capabilities of Cortex XSIAM be used on the data?

A. Create a behavioral indicator of compromise (BIOC) rule on the network fields (source IP, source port, target IP, target port. IP protocol).

B. Create a data model rule with network fields mapped (source IP. source port, target IP. target port. IP protocol).

C. Create a correlation rule on the network fields (source IP. source port, target IP. target port. IP protocol).

D. Create a parsing rule and ensure the network fields exist (source IP. source port, target IP. target port. IP protocol).

Answer: B

Explanation:

To leverage Cortex XSIAM analytics on custom-ingested firewall data, a data model rule must be created with the key network fields (source IP, source port, target IP, target port, IP protocol) mapped. This enables the data to align with XSIAM's analytics engine and be used for BIOCs, correlation rules, and advanced detections.

Question: 12

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: B, C

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: 13

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: 14

What should be considered when creating a custom incident domain?

A. Alert grouping will not apply, but SmartScore will.

B. Alert grouping will apply, but SmartScore will not.

C. Alert grouping and SmartScore will not be applied to incidents.

D. Alert grouping and SmartScore will be applied to incidents.

Answer: B

Explanation:

When creating a custom incident domain in Cortex XSIAM, alert grouping still applies, allowing related alerts to be combined into incidents. However, SmartScore is not applied, since it is reserved for predefined domains.

Question: 15

How does Cortex XSIAM manage licensing for Kubernetes environments?

A. Managed per namespace and returned when the namespace is decommissioned

B. Issued per container and returned upon container termination

C. Issued for each node and returned when the agent is removed or the node is deleted

D. Applied per service deployment and returned upon service deactivation

Answer: C

Explanation:

In Kubernetes environments, Cortex XSIAM licensing is issued per node. The license is consumed when the agent is installed on a node and is automatically returned when the agent is removed or the node is deleted, ensuring accurate license utilization.

Question: 16

A Cortex XSIAM engineer is preparing to install a new content pack and notices that there are several optional content packs associated with the main one that needs to be installed.

What must the engineer take into consideration when deciding whether or not to install the optional content packs?

A. Mandatory dependencies required by the optional content packs are automatically included during installation. The engineer should consider the additional functionality and potential impact on system performance.

B. The optional content packs without their associated dependencies are installed first, and then the main content pack installation is triggered. The engineer should ensure that the optional content packs do not conflict with existing configurations.

C. Optional content packs are installed without any dependencies, as they are not necessary. The engineer should only install them if they require the additional features.

D. Only the selected optional content packs are installed, without including any additional dependencies. The engineer should manually check for any required dependencies.

Answer: A

Explanation:

When installing optional content packs in Cortex XSIAM, any mandatory dependencies are automatically included. The engineer's main consideration is whether the additional functionality is needed and whether it may have a performance impact on the system.

Question: 17

In the Incident War Room, which command is used to update incident fields identified in the incident layout?

A. !setIncidentFields

B. !setParentIncidentFields

C. !setParentIncidentContext

D. !updateParentIncidentFields

Answer: A

Explanation:

The !setIncidentFields command is used in the Incident War Room to directly update incident fields that are defined in the incident layout, ensuring the incident record reflects the latest information.

Question: 18

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

Context Data

H I

customJields: { incidentassignment: {

runStatus: mi .

start Date: 2< 2 5 01)8 U • •

58)

Table

runStatus running

startDate 2025-01-08 18:44:1

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:

The correct command is !ToTable data=${parentIncidentFields.custom_fields.incidentassignment}, which converts the specified context data into a tabular format. This allows fields such as runStatus and startDate to be clearly displayed in a table when troubleshooting playbook tasks.

Question: 19

What is the role of "in" in the query line below?

action_local_port in (1122, 2234)

A. Operand

B. Operator

C. Function

D. Range

Answer: B

Explanation:

In the query action_local_port in (1122, 2234), the word "in" functions as an operator. It checks whether the field action_local_port matches any value in the specified list (1122, 2234).

Question: 20

Which section of a parsing rule defines the newly created dataset?

A. RULE

B. COLLECT

C. INGEST

D. CONST

Answer: B

Explanation:

In a Cortex XSIAM parsing rule, the COLLECT section defines the newly created dataset. This section specifies how the parsed fields and data should be structured and stored for further use in analytics and queries.

Question: 21

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: 22

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)

I

```
dataset • va eves
    filter affect^d product3 contains "ai app"
 I fields affected hosts, affected products
```

B)

dataset - xdr data
I filter event type = EN”M.PROCESS
I filter actionjirocesaimaqename = "ai_app"
I filter action jprocess’fileinfo not in ("12.1”, "12.2", "12 J", "’2.5")

C)

preset ■ ho3t_inventory_applications
I filter applicationname contains "ai app" and version in ("12.1", "12.2", "12.4", "12.5")

D)

dataset * host inventory
I filter applicationNane contains "ai app"
I filter applicationversion not in ("12.1", ”12.2", "12.4", "12.5")

A. Option A

B. Option B

C. Option C

D. Option D

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: 23

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: 24

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: 25

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 postingestion 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-ingestion for necessary transformations and integrity checks.

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 postingestion. This ensures that threat detection and response are based on unaltered, high-fidelity data while still enabling normalization and enrichment after ingestion.

Question: 26

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: 27

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: 28

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.

Question: 29

What is the function of the "MODEL" section when creating a data model rule?

A. To make a list of all the relevant fields to be mapped from the logs to XDM

B. To define the mapping between a single dataset and XDM

C. To finalize rule definition with all XQL statements

D. To map log fields to corresponding Cortex XSIAM Data Model (XDM) fields

Answer: D

Explanation:

The MODEL section in a data model rule is used to map log fields to the corresponding Cortex XSIAM Data Model (XDM) fields. This ensures that ingested data aligns with XDM, enabling consistent analytics, detections, and queries across different data sources.

Question: 30

What is the primary benefit of setting the "--memory-swap" option to "-1" during Cortex XSIAM engine deployment?

A. It enhances the network throughput by optimizing memory usage.

B. It increases the total disk space available to the engine.

C. It allows the engine to operate without requiring swap capabilities.

D. It automatically doubles the available RAM to the engine.

Answer: C

Explanation:

Setting the "--memory-swap" option to "-1" during Cortex XSIAM engine deployment configures the container to run without requiring swap capabilities. This ensures the engine operates fully within allocated RAM, improving stability and avoiding issues related to memory swapping.

Question: 31

A CISO has asked an engineer to create a custom dashboard in Cortex XSIAM that can be filtered to show incidents assigned to a specific user.

Which feature should be used to filter the incident data in the dashboard?

A. Filters and inputs in the custom dashboard

B. Report template to set the incident user filter

C. Visualization filter options in the widget configuration

D. Incident summary view to filter by user

Answer: A

Explanation:

To show incidents assigned to a specific user in a Cortex XSIAM custom dashboard, the engineer should use filters and inputs in the custom dashboard. This enables dynamic filtering of incident data, allowing the dashboard to be customized based on user assignment.

Question: 32

How can a Cortex XSIAM engineer resolve the issue when a SOC analyst escalates missing details after merging two similar incidents?

A. Check the War Room of the destination incident.

B. Examine the incident context of the source incident.

C. Unmerge the incidents and copy the missing details into the incident notes.

D. Check the child incident of the destination incident.

Answer: A

Explanation:

When two incidents are merged in Cortex XSIAM, the War Room of the destination incident retains the merged details and activity logs. If a SOC analyst reports missing details, checking the destination incident's War Room will provide the complete context and history.

Question: 33

Which cytool command will look up the policy being applied to a Cortex XDR agent?

A. cytool adaptive_policy interval 0

B. cytool payload_execution query

C. cytool adaptive_policy recalc

D. cytool persist print agent_settings.db

Answer: C

Explanation:

The cytool adaptive_policy recalc command is used to look up and recalculate the policy being applied to a Cortex XDR agent, allowing engineers to verify the active policy enforcement on the endpoint.

Question: 34

A file for a support exception that needs to be updated locally on a Linux endpoint has been supplied.

Which cytool command will upload this support exception file to the endpoint?

A. cytool upload suexfile -target </local/file/path>

B. cytool upload suex -file </local/file/path>

C. cytool import suex -path </local/file/path>

D. cytool import suexfile -path </local/file/path>

Answer: C

Explanation:

The correct command is cytool import suex -path </local/file/path>, which imports a supplied support exception (suex) file onto a Linux endpoint, ensuring the exception is applied locally.

Question: 35

Using the integrationContext object, how is data stored and retrieved between integration command runs in Cortex XSIAM?

A. The integrationContex object can only store strings, not key-value dictionaries.

B. The integrationContex object is retrieved and set using the test-module command.

C. The get_integration_context() method overrides the existing object that is stored.

D. The integrationContex object supports get_integration_context() and set_integration_context().

Answer: D

Explanation:

The integrationContext object in Cortex XSIAM is persistent across integration command runs and is managed using get_integration_context() and set_integration_context(). This allows data (such as key-value dictionaries) to be stored and retrieved reliably between executions.

Question: 36

Which types of content may be included in a Marketplace content pack?

A. Integrations, playbooks, parsers, and server configuration keys

B. Predefined dashboards, indicators, and reports

C. Scripts, playbooks, integrations, and correlation rules

D. Behavioral indicator of compromise (BIOC) rules, layouts, and custom dashboards

Answer: C

Explanation:

A Marketplace content pack in Cortex XSIAM can include scripts, playbooks, integrations, and correlation rules. These packaged content items extend platform functionality, automate workflows, and enhance detection and response capabilities.

Question: 37

Cortex XSIAM has not received any logs for 30 minutes from a Palo Alto Networks NGFW named "MainFW." An engineer wants to create an alert for this scenario.

Correlation rule settings include:

- Time Schedule: Every 30 minutes
- Query Timeframe: 30 minutes
- Action: Generate alert
- Alert Name: No logs received from MainFW in the past 30 minutes

Which query should be used in the correlation rule?

A)

dataset - collection auditing
filter collector type = "NGFW" and instance = "MainFW*
I comp countdistinct(description) as totalevents by instance filter total events • 0

B)

preset = metrics view

filter vendor "PANS" and _product - "NGFW" and _reporting_device_name - "Main I comp count_distinct(total_event_count) as total_events by _reporting_device_name I filter total events = 0

C)

dataset - collection auditing
| filter collector_type ■ "NGFW" and instance » "MainFW"
I comp values(description) as total events by instance
I filter total event® - 0

D)

preset = metrics view
filter vender "FANM" and product "NGFW" and reportingdevice—name ■ "Main I comp sum(total_event_count) as totalevents by reporting device name
I filter total events - 0

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

The correct query is the one using preset = metrics_view with

comp sum(total_event_count) as total_events by _reporting_device_name and filtering total_events = 0.

This query directly checks event counts reported by the NGFW ("MainFW"). If no logs are received in the last 30 minutes, the total event count will be 0, which triggers the correlation rule alert.

Question: 38

A Cortex XSIAM engineer at a SOC downgrades a critical threat intelligence content pack from the Cortex Marketplace while performing routine maintenance. As a result, the SOC team loses access to the latest threat intelligence data.

Which action will restore the functionality of the content pack to its previously installed version?

A. Contact Palo Alto Networks Support to create an exception to revert to the previously installed version.

B. Back up the current configuration and data, then revert to the previously installed version.

C. Remove all integrations and playbooks associated with the content pack, then revert to the previously installed version.

D. Directly reinstall the previously installed version over the current one.

Answer: D

Explanation:

To restore the content pack to its previously installed version, the engineer can directly reinstall the desired version from the Cortex Marketplace. Content packs support version management, allowing rollback or upgrade without requiring support intervention or removing existing configurations.

Question: 39

Which two alert notification options can be configured without creating a playbook? (Choose two.)

Which two alert notification options can be configured without creating a playbook? (Choose two.)

A. Pager Duty

B. Email

C. Slack

D. SMS

Answer: B, C

Explanation:

Cortex XSIAM allows configuring Email and Slack as direct alert notification options without requiring a playbook. PagerDuty and SMS integrations, however, require orchestration through playbooks.

Question: 40

An engineer needs to migrate Cortex XDR agents without internet connection from Cortex XSIAM tenant A to Cortex XSIAM tenant B. There is a broker configured for each tenant. This is the communication flow:

XDR agents <-> Broker A <-> XSIAM tenant A

XDR agents <-> Broker B <-> XSIAM tenant B

Which two steps should be taken before moving the agents? (Choose two.)

A. Install a new Broker C on site B, and register it into Cortex XSIAM tenant A.

B. Install a new Broker C on site and register it into Cortex XSIAM tenant B.

C. Also register Broker A to Cortex XSIAM tenant B.

D. Select all endpoints in the console and add a new Broker C as proxy.

Answer: B, C

Explanation:

To migrate XDR agents without internet from tenant A to tenant B, the engineer must install a new Broker C registered to tenant B to establish communication, and also register Broker A with tenant B so existing agents can transition their communication path smoothly during migration.

Question: 41

Which field is automatically mapped from the dataset to the data model when creating a data model rule?

A. _event_type

B. _insert_time

C. _host_name

D. _cloud_id

Answer: A

Explanation:

When creating a data model rule, the field _event_type is automatically mapped from the dataset to the data model. This ensures events are categorized correctly in alignment with the Cortex XSIAM Data Model (XDM).

Question: 42

A Cortex XSIAM engineer plans to add Kafka and Syslog Collectors to a Broker VM cluster.

What are two expected behaviors of the applets when they are added to the cluster? (Choose two.)

A. Syslog Collector applet is automatically initiated, enters an active state on the primary node, and is on standby on the standby nodes.

B. Kafka Collector applet is automatically initiated, enters an active state on the primary node, and is on standby on the standby nodes.

C. Syslog Collector applet is active on all cluster nodes, including primary and standby.

D. Kafka Collector applet is active on all cluster nodes, including primary and standby.

Answer: A, D

Explanation:

In a Broker VM cluster, the Syslog Collector applet runs in active/standby mode (active on the primary node, standby on others), while the Kafka Collector applet runs in active/active mode (active on all nodes). This design ensures both high availability and scalability for ingestion.

Question: 43

Based on the _raw_log and XQL query information below, what will be the result(s) of the temp_value?

raw log:

```
2(22-0) 17 01 17 $9.917200 iour<*:149 23$ 219.290 port:$]9M Urpt: 19.120 M 2 port42) up 1794 dow> $9) duration-9 «»MNl*
2122 0) 17 0139:29.197424 twrct:121. 14.142.2)5 port:59977 Urgct 10.120.M.4 oort:29 uc:2277 dc^:1215 dur<tlon:0 ircondt
```

XQL query

```
t**p_vih« a l                    (    (_r*._lof, •(W(l.»\.W(l,J)tW(i,J)\.\4{l,>))•), 0) ~ "MOtHS*. •■
( t(_ra._lH. *W(M)\.\0{lJ)\.14(l,J}\.W(l.l)\ipert\ (\d»D. JJ.'Ml.ia 10.1*)
```

A. 123
192.168.10.1

B. 20

C. 10.120.80.2

D. 149.235.219.208
59977

Answer: A

Explanation:

The XQL query uses regextract with conditions to check if the source IP begins with 149.235. When true, it assigns the replacement value 192.168.10.1, otherwise it extracts the source port. From the given logs, this produces 123 (from the port

extraction in the second log) and 192.168.10.1 (replacement for the first log's matching source IP).

Question: 44

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: B

Explanation:

During Cortex XSIAM tenant activation, data at rest is configured with AES 128 encryption by selecting "BYOK" (Bring Your Own Key) under the Advanced → Encryption Method option and following the wizard's instructions. This ensures secure key management and compliance with encryption standards.

Question: 45

A sub-playbook is configured to loop with a For Each Input. The following inputs are given to the subplaybook:

Input x: W,X,Y,Z

Input y: a,b,c,d

Input z: 9

Which inputs will be used for the second iteration of the loop?

A. a,b,c,d

B. X,b,9

C. X,b

D. X,b,c

Answer: B

Explanation:

In a For Each Input loop, each iteration takes the next value from the list inputs while keeping constant inputs unchanged.

On the second iteration:

- x = X (second value of W,X,Y,Z)
- y = b (second value of a,b,c,d)
- z = 9 (constant for all iterations).

So, the values are X, b, 9.

Question: 46

The following string is a value of a key named "Data2" in the context:

{"@admin":"admin","@dirtyId":"1","@loc":"Lab","@name":"default- 1","@oldname":"Test","@time":"2024/08/28 07:45:15","alert":{"@admin":"admin","@dirtyId":"2","@time":"2024/08/28 07:45:15","member":{"#text":"

Based on the image below, what will be displayed in the "Test result" field when the "Test" button is pressed?

A. 1

B. "1

C. 2

D. "2

Answer: B

Explanation:

The applied transformers extract the value of @dirtyId from the root-level Data2 object. The sequence includes trimming using "Id:" and ending with a quotation mark ". As a result, the root @dirtyId value (1) is returned with a leading quotation mark, so the Test result will display "1.

Question: 47

A Cortex XDR agent is installed on an endpoint, but the agent is unable to download content updates and has not registered with the Cortex XSIAM server. An engineer troubleshoots the network connection and determines that, by design, this endpoint does not have direct internet access to the required network destinations for the Cortex XDR agent traffic.

A Broker VM that has the local agent settings applet enabled with Agent Proxy configured is

reachable by the endpoint. The Broker VM details are as follows:

FQDN: crtxbroker01.company.net

Proxy listening port: 8888

How should the engineer configure the Cortex XDR agent to use the existing Broker VM as a proxy for the agent network traffic?

A. cytool proxy set "crtxbroker01. company.net: 8888"

B. cytool config proxy --host crtxbroker01.company.net --port 8888

C. cytool set proxy --host crtxbroker01.company.net --port 8888

D. cytool proxy config "crtxbroker01.company.net:8888"

Answer: B

Explanation:

The correct command is cytool config proxy --host crtxbroker01.company.net --port 8888, which configures the Cortex XDR agent to route its traffic through the Broker VM acting as a proxy. This allows the agent to register and download updates without requiring direct internet access.

Question: 48

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:

- Platform: Windows
- Target Properties: SHA256, File path, Microsoft Corporation
- Module: Behavioral Threat Protection
- Scope: Exceptions-AppServers

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

- Platform: Windows
- Target Properties: C:\Windows\System32\cmd exe
- Module: Behavioral Threat Protection
- Profiles: Malware-AppServers

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:

The most secure approach is to create a Disable Prevention Rule via Exceptions Configuration, scoped specifically to the Exceptions-AppServers profile. This rule should include the hash (SHA256), signer (Microsoft Corporation), and file path (C:\Windows\System32\cmd.exe). This ensures the exception is applied only to the trusted, legitimate process on the AppServers group while minimizing the security gap.

Question: 49

Which action will prevent the automatic extraction of indicators such as IP addresses and URLs from a script's output?

A. Add 'ExtractIndicators': False to the script.

B. Add 'IgnoreAutoExtract': True to the script.

C. Use 'AutoExtract': False in the script.

D. Set 'IndicatorExtraction': None in the script.

Answer: C

Explanation:

To prevent Cortex XSIAM from automatically extracting indicators (like IPs, domains, and URLs) from a script's output, you must use 'AutoExtract': False in the script. This disables the auto-extraction mechanism for that script.

Question: 50

An application which ingests custom application logs is hosted in an on-premises virtual environment on an Ubuntu server, and it logs locally to a .csv file.

Which set of actions will allow the ingestion of the .csv logs into Cortex XSIAM directly from the server?

An application which ingests custom application logs is hosted in an on-premises virtual environment on an Ubuntu server, and it logs locally to a .csv file.

Which set of actions will allow the ingestion of the .csv logs into Cortex XSIAM directly from the server?

A. Install a Broker VM in the environment, and configure the CSV Collector to collect the files of interest.

B. Install a Cortex XDR agent on the Ubuntu server, and configure the agent to collect the files of interest.

C. Install a Broker VM in the environment, and migrate the application to the Broker VM.

D. Install XDR Collector on the Ubuntu server, and configure the agent to collect the files of interest.

Answer: A

Explanation:

The correct approach is to install a Broker VM in the environment and configure its CSV Collector applet to ingest the .csv log files directly from the Ubuntu server. This enables secure ingestion of custom application logs into Cortex XSIAM without modifying the application or requiring an XDR agent on the server.

Question: 51

Which action is required to enable use of a custom script in an alert layout?

A. Tag the script with "dynamic-section," add a general purpose dynamic section, and edit the section settings to add the automation script.

B. Tag the script with "general-purpose-dynamic-section," add a custom script section, and edit the section

settings to add the automation script.

C. Add a general purpose dynamic section and edit the section settings to add the automation script.

D. Tag the script with "general-purpose-dynamic-section." add a general purpose dynamic section, and edit the section settings to add the automation script.

Answer: D

Explanation:

To use a custom script in an alert layout, the script must be tagged with "general-purpose-dynamicsection", then a general purpose dynamic section is added to the layout, and finally the section settings are edited to attach the automation script. This ensures the script executes and displays results dynamically within the alert layout.

Question: 52

What is the reason all Broker VM options are greyed out when a user attempts to select a Broker VM as a download source in the Agent Settings profile?

A. The Broker VM is ofline.

B. NTP is not synchronized properly on the Broker VM.

C. Local Agent Setting applet is currently activated without SSL certificate.

D. Local Agent Setting applet is currently activated without FQDN.

Answer: D

Explanation:

Broker VM options appear greyed out in the Agent Settings profile when the Local Agent Settings applet is activated without an FQDN. An FQDN is required for agents to resolve and connect to the Broker VM as a download source.

Question: 53

What is a key characteristic of a parsing rule in Cortex XSIAM?

A. It uses regular expressions exclusively for data modifications, discards unmatched logs by default, and only retains fields with non-null values.

B. It is bound to all vendors and products, performs data parsing once per log, and does not allow

grouping.

C. It is bound to a specific vendor and product, performs data parsing once per log, and does not allow grouping.

D. It is bound to a specific vendor and product which allow grouping with a no-match policy, and retains all fields.

Answer: C

Explanation:

A parsing rule in Cortex XSIAM is bound to a specific vendor and product, ensuring accurate parsing logic for that log source. It processes each log individually (once per log) and does not allow grouping, making it distinct from data model rules.

Question: 54

Which type of parsing error is categorized in the dataset "parsing_rules_errors"?

A. Compilation

B. Unrecognized code

C. Invalid syntax

D. Data mismatch

Answer: A

Explanation:

The parsing_rules_errors dataset records compilation errors that occur when a parsing rule cannot be properly built or executed. This helps engineers identify and fix issues in rule definitions before logs are processed.

Question: 55

Before initiating a malware scan action on a Linux workstation, an engineer notices that the Cortex XDR agent's operational status on the workstation is reporting as "partially protected." There have been no configuration changes made from the Cortex XSIAM server.

What are two explanations for this operational status? (Choose two.)

A. The Linux endpoint is currently running 4.0 kernel version.

B. The Linux endpoint's kernel modules failed to load due to unsupported kernel versions.

C. The agent is outdated and requires an upgrade to the latest version to regain full protection.

D. The agent was manually disabled on the endpoint by the user or an administrator.

Answer: B, C

Explanation:

The "partially protected" status on a Linux endpoint typically occurs when the kernel modules fail to load because of unsupported kernel versions or when the agent is outdated and requires an upgrade. Both conditions prevent the agent from providing full protection capabilities.

Question: 56

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:

To meet the requirements, the engineer must enable scope enforcement by setting SBAC mode to Restrictive and assigning the Europe endpoint group (EG:Europe) as the scope. For role assignment, the correct predefined role is Privileged IT Admin, since it allows endpoint management, policy creation, and Live Terminal but does not permit user role management.

Question: 57

Administrators from Building 3 have been added to Cortex XSIAM to perform limited functions on a subset of endpoints. Custom roles have been created and applied to the administrators to limit their permissions, but their access should also be constrained through the principle of least privilege according to the endpoints they are allowed to manage. All endpoints are part of an endpoint group named "Building3," and some endpoints may also be members of other endpoint groups.

Which technical control will restrict the ability of the administrators to manage endpoints outside of their area of responsibility, while maintaining visibility to Building 3's endpoints?

A. SBAC enabled in Building 3's IP range with the "EG:Building3" tag assigned to each administrator's scope

B. SBAC enabled in Permissive Mode with the "EG:Building3" tag assigned to each administrator's scope

C. SBAC enabled in Restrictive Mode with the "EG:Building3" tag assigned to each administrator's scope

D. SBAC enabled globally with the "EG:Building3" tag assigned to each administrator's scope

Answer: C

Explanation:

To enforce least privilege for Building 3 administrators, SBAC must be enabled in Restrictive Mode and the administrators' scope must be limited to EG:Building3. This ensures they can only manage endpoints within the Building 3 group, even if those endpoints are also part of other groups, while blocking access to endpoints outside their responsibility.

Question: 58

While using the playbook debugger, an engineer attaches the context of an alert as test data.

What happens with respect to the interactions with the list objects via tasks in this scenario?

A. The original content of the list and the original context are not altered, because Cortex XSIAM is running

inside debug mode.

B. The original content of the list is not altered, but the original context is, because XSIAM commands are running within debug mode.

C. The original content of the list is altered, but the original context is not, because Cortex XSIAM commands interact directly with the original list objects within debug mode.

D. The original content of the list and the original context are altered, because Cortex XSIAM tasks interact directly with the objects, even within debug mode.

Answer: A

Explanation:

When running the playbook debugger with attached test data, Cortex XSIAM operates entirely in debug mode, meaning neither the original list objects nor the original context are altered. All interactions happen in an isolated debug environment to avoid impacting production data.

Question: 59

What is the primary function of the URL "https://<region>-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 https://<region>-docker.pkg.dev is used in Palo Alto Networks infrastructure to download Engine Docker containers. This ensures the Cortex XSIAM engine components are pulled securely from the regional Docker registry.