Question #1 *Topic 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.

Suggested Answer: *B*

Community vote distribution

B (100%)

ureyes968 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Johfor 2 months ago

Selected Answer: B

This is correct

upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *BC*

Community vote distribution

BC (75%) BD (25%)

Bradl 1 month, 2 weeks ago

Selected Answer: BD

BD, You can monitor correlation rule executions (including failures) via the correlations_auditing and Cortex XSIAM also raises OOTB Health (DOMAIN_HEALTH) alerts when a correlation rule completes with an error status.

upvoted 1 times

ureyes968 1 month, 2 weeks ago

Selected Answer: BC

bc is correct

upvoted 1 times

CKiel 2 months, 1 week ago

Selected Answer: BD

BD is correct. D: Cortex comes with OOTB health issues generated when correlation rule completes with error.

upvoted 1 times

youknowz 4 months, 3 weeks ago

Selected Answer: BC

XDR Collector audit logs don't have a type=Rules. Also, why would the collector have anything to do with a rule internal to XSIAM?

upvoted 3 times

Question #3 *Topic 1*

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

Suggested Answer: *B*

ureyes968 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Question #4 *Topic 1*

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

Suggested Answer: *C*

ureyes968 1 month, 2 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

Question #5

Topic 1

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.

Suggested Answer: *D*

ureyes968 1 month, 2 weeks ago

Selected Answer: D

d is correct

upvoted 1 times

Question #6 Topic 1

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. Lists

D. Layouts

Suggested Answer: *AC*

Community vote distribution

AD (100%)

evilCorpBot7494 3 days, 19 hours ago

Selected Answer: AD

Scripts and layouts, apart from Alert types and fields, Indicator types and fields, Alert and indicator layouts, Classifiers, Integrations, Playbooks

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Documentation/Cortex-XSIAM-development-tenant#:~:text=content%20types%20are-,push/pull%20supported,-%3A

upvoted 1 times

ureyes968 1 month, 2 weeks ago

Selected Answer: AC

When using a remote repository on a Development Cortex XSIAM tenant, only certain content objects are supported for push/pull operations. These include:

Scripts → Custom automation logic can be versioned and synchronized.

Lists → Used for lookups, allowlists/blocklists, and enrichment data, and can also be synced via the repository.

upvoted 1 times

CKiel 2 months, 1 week ago

Selected Answer: AD

AD is correct

upvoted 1 times

Question #7 *Topic 1*

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.

Suggested Answer: *BD*

ureyes968 1 month, 2 weeks ago

Selected Answer: BD

bd is correct

upvoted 1 times

Question #8 *Topic 1*

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

Suggested Answer: *B*

Arbehueh 1 month, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

ureyes968 1 month, 1 week ago

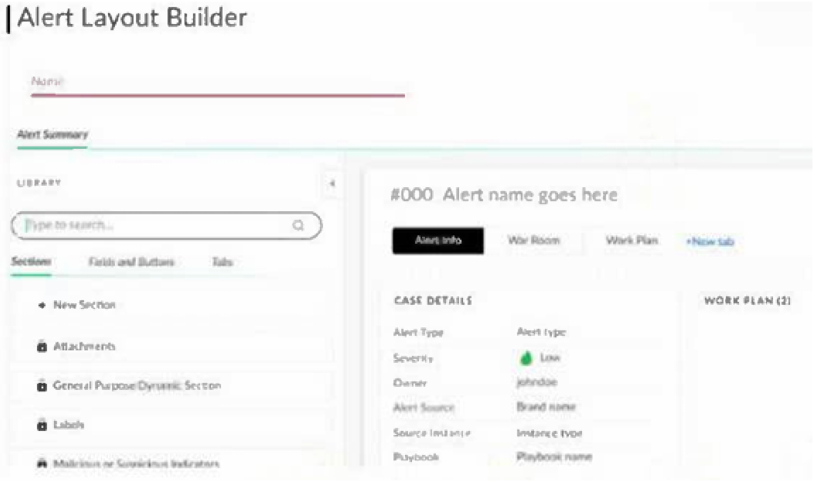
Selected Answer: B

B is correct

upvoted 1 times

Question #9 Topic 1

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



Alert Type	Alert type
Severity	Low
Owner	johndoe
Alert Source	Brand name
Source Instance	Instance type
Playbook	Playbook name

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

ureyes968 1 month, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

davidpm 2 months, 3 weeks ago

Selected Answer: A

correct, only alert info

upvoted 1 times

darylmaeb24 5 months, 1 week ago

Selected Answer: A

only alert info can be deleted

upvoted 3 times

Question #10 *Topic 1*

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.

Suggested Answer: *B*

⊟ **ureyes968** 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Question #11 *Topic 1*

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).

Suggested Answer: *B*

ureyes968 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Question #12 *Topic 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.

Suggested Answer: *BC*

ureyes968 1 month, 2 weeks ago

Selected Answer: BC

b,c correct

upvoted 1 times

Question #13 *Topic 1*

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.

Suggested Answer: *B*

ureyes968 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Question #14 *Topic 1*

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.

Suggested Answer: *B*

ureyes968 1 month, 2 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

> **ureyes968** 3 weeks, 6 days ago
>
> sorry, B is correct
>
> upvoted 1 times

Question #15 *Topic 1*

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

Suggested Answer: *C*

ureyes968 1 month, 2 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

Question #16 *Topic 1*

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.

Suggested Answer: *A*

ureyes968 1 month, 2 weeks ago

Selected Answer: A

a is correct

upvoted 1 times

Question #17 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

B (100%)

ureyes968 1 month, 2 weeks ago

Selected Answer: A

a is correct
In the Incident War Room (Cortex XSIAM / XSOAR), the command used to update incident fields that are defined in the incident layout is:

!setIncidentFields

This command:

Updates incident-level fields

Reflects immediately in the incident layout
Is commonly used in playbooks and manual War Room actions
upvoted 1 times

davidpm 1 month, 3 weeks ago

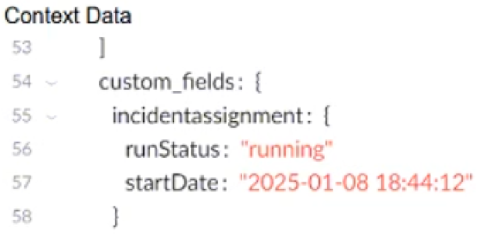
Selected Answer: B

B. !setParentIncidentFields
upvoted 1 times

Question #18

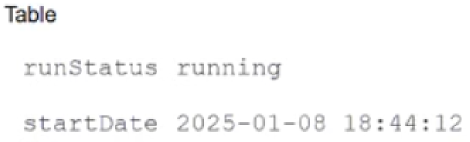
Topic 1

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

```
    ]
    custom_fields: {
      incidentassignment: {
        runStatus: "running"
        startDate: "2025-01-08 18:44:12"
      }
```



Table

```
runStatus running

startDate 2025-01-08 18:44:12
```

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}

Suggested Answer: *C*

⊟ **ureyes968** 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Question #19 *Topic 1*

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

Suggested Answer: *B*

ureyes968 1 month, 2 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

Question #20 *Topic 1*

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

A. RULE

B. COLLECT

C. INGEST

D. CONST

Suggested Answer: *B*

Community vote distribution

C (100%)

ureyes968 1 month, 2 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

davidpm 1 month, 4 weeks ago

Selected Answer: C

INGEST Section: This header defines the metadata for the logs, specifically the vendor, product, and the target_dataset (the name of the newly created or destination dataset). It acts as the entry point that tells the system where to route the data.

COLLECT Section: Used specifically for data reduction and manipulation at the Broker VM level (e.g., filtering events before they are sent to the cloud), not for defining the final XSIAM storage dataset.

upvoted 1 times

Question #21 *Topic 1*

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.

Suggested Answer: *C*

⊟ **ureyes968** 1 month, 2 weeks ago

Selected Answer: C

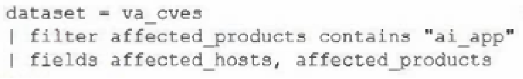
c is correct

upvoted 1 times

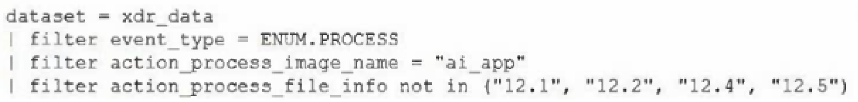
Question #22 *Topic 1*

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.

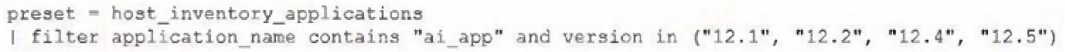
Which XQL query will provide the required result?

A. 

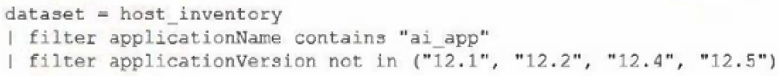
```
dataset = va_cves
| filter affected_products contains "ai_app"
| fields affected_hosts, affected_products
```

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")
```

Suggested Answer: *C*

ureyes968 1 month, 2 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

Question #23 *Topic 1*

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

Suggested Answer: *B*

⊟ **ureyes968** 1 month ago

Selected Answer: B

b is correct

upvoted 1 times

Question #24 *Topic 1*

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

A. Standalone

B. Helm

C. Upgrade from ESM

D. Kubernetes

Suggested Answer: *B*

Community vote distribution

A (100%)

davidpm 1 month, 3 weeks ago

Selected Answer: A

Helm is for linux only. Correct answer is Standalone for Windows

upvoted 1 times

Question #25 *Topic 1*

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-ingestion for necessary transformations and integrity checks.

Suggested Answer: *D*

ureyes968 1 month, 2 weeks ago

Selected Answer: D

d is correct

upvoted 1 times

Question #26 *Topic 1*

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

Suggested Answer: *A*

ureyes968 1 month, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

Question #27 *Topic 1*

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.

Suggested Answer: *B*

ureyes968 1 month, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

Question #28 *Topic 1*

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.

Suggested Answer: *A*

ureyes968 1 month, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

Question #29 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

B (100%)

ureyes968 1 month, 1 week ago

Selected Answer: D

When creating a data model rule in Cortex XSIAM, the MODEL section is specifically used to:Define how fields from the ingested logs are mapped to standardized XDM fields

Ensure data from different sources is normalized into a common schema (XDM) so it can be correlated, searched, and analyzed consistently

upvoted 1 times

davidpm 1 month, 3 weeks ago

Selected Answer: B

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Documentation/MODEL

upvoted 1 times