Question #1 *Topic 1*

Which dataset should an analyst search when looking for Palo Alto Networks NGFW logs?

A. dataset = pan_dss_raw

B. dataset = ngfw_threat_panw_raw

C. dataset = panw_ngfw_traffic_raw

D. dataset = ngfw*

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 Topic 1

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

A. Feed Integration settings

B. Indicator Configuration in Object Setup

C. STIX parser code

D. Classification & Mapping tab

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

An analyst conducting a threat hunt needs to collect multiple files from various endpoints. The analyst begins the file retrieval process by using the Action Center, but upon review of the retrieved files, notices that the list is incomplete and missing files, including kernel files.
What could be the reason for this issue?

A. The file retrieval policy applied to the endpoints may restrict access to certain system or kernel files.

B. The retrieval process is limited to 500 MB in total file size.

C. The endpoint agents were in offline mode during the file retrieval process, causing some files to be skipped.

D. The analyst must manually retrieve kernel files by accessing the machine directly.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Which interval is the duration of time before an analytics detector can raise an alert?

A. Activation period
B. Deduplication period
C. Training period
D. Test period

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which two actions can an analyst take to reduce the number of false positive alerts generated by a custom BIOC? (Choose two.)

A. Implement a BIOC rule exception.

B. Implement a global exception in the prevention profile.

C. Implement an alert exclusion rule.

D. Implement a shunt in a BIOC bypass rule.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #6

Topic 1

For a critical incident, Cortex XSIAM suggests several playbooks which should have been executed automatically.
Why were the playbooks not executed?

A. Playbook triggers were not configured for those alerts.

B. Installation of the appropriate content pack was not completed.

C. Misconfiguration of the connector instance has occurred.

D. Playbook classifier was not configured for the alert type.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

What information is provided in the timeline view of Cortex XSIAM?

A. Graphic representation of an event Causality Instance (CI) with additional capabilities to enable further analysis

B. Sequence of events, alerts, rules, and other actions involved over the lifespan of an incident

C. Tab within an incident where analysts can collaborate and initiate further actions and automations

D. Detailed overview of behavior or activity that triggered an Analytics Alert, Analytics BIOC alert, or correlation rule

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which two methods can be used to create and share queries into the Query Library? (Choose two.)

A. From XQL Search, locate the query to save to a personal Query Library
Right-click, and select "Save query to library"
Enable the "Share with others" option

B. From the Query Center, in the XQL query field, define the parameters of the query
Save as, and choose the "Query to Library" option
Enable the "Share with others" option

C. From XQL Search, in the XQL query field, define the parameters of the query
Save as, and choose the "Query to Library" option
Enable the "Share with others" option

D. From the Query Center, locate the query to save to a personal Query Library
Right-click, and select "Save query to library"
Enable the "Share with others" option

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Which type of task can be used to create a decision tree in a playbook?

A. Sub-playbook

B. Job

C. Standard

D. Conditional

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

A Cortex XSIAM analyst is investigating a security incident involving a workstation after having deployed a Cortex XDR agent for 45 days. The incident details include the Cortex XDR Analytics Alert "Uncommon remote scheduled task creation."
Which response will mitigate the threat?

A. Revoke user access and conduct a user audit.

B. Allow list the processes to reduce alert noise.

C. Initiate the endpoint isolate action to contain the threat.

D. Prioritize blocking the source IP address to prevent further login attempts.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which Cytool command will re-enable protection on an endpoint that has Cortex XDR agent protection paused?

A. cytool security enable

B. cytool service start

C. cytool runtime start

D. cytool protect enable

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12

Topic 1

A Cortex XSIAM analyst is reading a blog that references an unfamiliar critical zero-day vulnerability. This vulnerability has been weaponized, and there is evidence that it is being exploited by threat actors targeting a customer's industry.
Where can the analyst go within Cortex XSIAM to learn more about this vulnerability and any potential impacts on the customer environment?

A. Threat Intel Management --> Sample Analysis

B. Attack Surface --> Threat Response Center

C. Attack Surface --> Attack Surface Rules

D. Threat Intel Management --> Indicator

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #13

Topic 1

While investigating an alert, an analyst notices that a URL indicator has a related alert from a previous incident. The related alert has the same URL, but it resolved to a different IP address.
Which combination of two actions should the analyst take to resolve this issue? (Choose two.)

A. Enrich the IP address indicator associated with the previous alert.
B. Expire the URL indicator.
C. Remove the relationship between the URL and the older IP address.
D. Enrich the URL indicator.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Which two actions will allow a security analyst to review updated commands from the core pack and interpret the results without altering the incident audit? (Choose two.)

A. Create a playbook with the commands and run it from within the War Room.

B. Run the core commands directly by typing them into the playground CLI.

C. Run the core commands directly from the Command and Scripts menu inside playground.

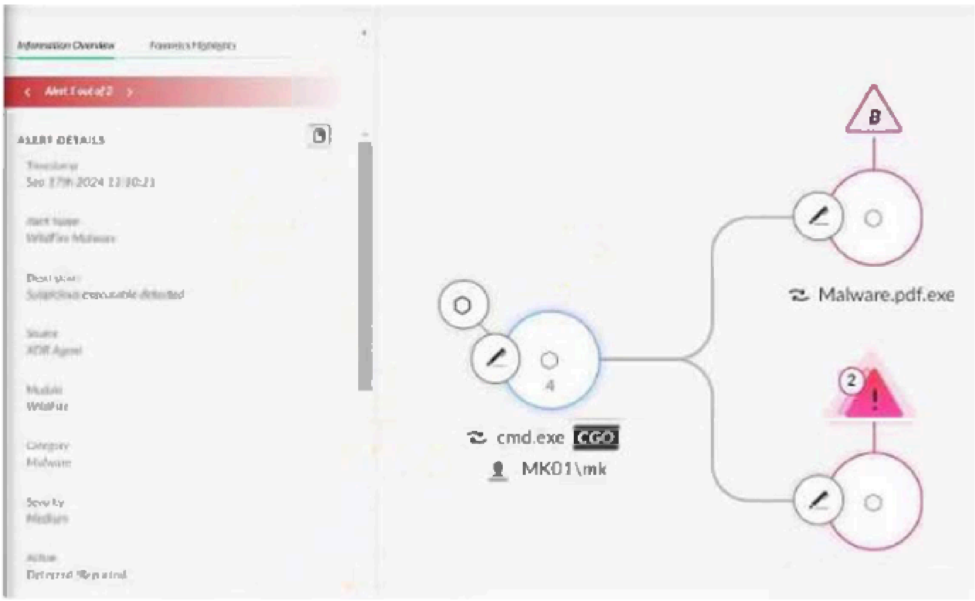
D. Run the core commands directly from the playground and invite other collaborators.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Based on the image below, which two determinations can be made from the causality chain? (Choose two.)



A. Three alerts in total were generated by the agent on the endpoint.

B. Cortex XDR agent malware profile module applied is set to "Report" mode.

C. Malware.pdf.exe is responsible for the entire chain of execution resulting in the alerts.

D. The process cmd.exe is responsible for the entire chain of execution resulting in the alerts.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

How can a SOC analyst highlight alerts generated on C-level executive hosts?

A. Add the C-level executive users to the Executive Accounts asset role.

B. Add a tag to the C-level executive users.

C. Create a Featured Alert field for the C-level hosts.

D. Create a dynamic group for the C-level hosts.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17

Topic 1

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

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

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

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

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 Topic 1

Which pane in the User Risk View will identify the country from which a user regularly logs in, based on the past few weeks of data?

A. Login Attempts

B. ACTUAL ACTIVITY

C. Latest Authentication Attempts

D. Common Locations

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which attributes can be used as featured fields?

A. Device-ID, URL, port, and indicator

B. CIDR range, file hash, tags, and log source

C. Endpoint-ID, alert source, critical asset, and threat name

D. Hostnames, user names, IP addresses, and Active Directory

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20

Topic 1

A SOC team member implements an incident starring configuration, but incidents created before this configuration were not starred.
What is the cause of this behavior?

A. The analyst must manually star incidents after determining which alerts within the incident were automatically starred.

B. Starring configuration is applied to the newly created alerts, and the incident is subsequently starred.

C. It takes 48 hours for the configuration to take effect.

D. Starring is applied to alerts after they have been merged into incidents, but incidents are not starred.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #21

Topic 1

An incident in Cortex XSIAM contains the following series of alerts:
10:24:17 AM - Informational Severity - XDR Analytics BIOC - Rare process execution in organization
10:24:18 AM - Low Severity - XDR BIOC - Suspicious AMSI DLL load location
10:24:20 AM - Medium Severity - XDR Agent - WildFire Malware
11:57:04 AM - High Severity - Correlation - Suspicious admin account creation
Which alert was responsible for the creation of the incident?

A. Rare process execution in organization

B. Suspicious admin account creation

C. WildFire Malware

D. Suspicious AMSI DLL load location

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which attribution evidence will have the lowest confidence level when evaluating assets to determine if they belong to an organization's attack surface?

A. An asset attributed to the organization because the Subject Organization field contains the company name

B. An asset attributed to the organization because the name server domain contains the company domain

C. An asset discovered through registration information attributed to the organization

D. An asset manually approved by a Cortex Xpanse analyst

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

When a sub-playbook loops, which task tab will allow an analyst to determine what data the sub-playbook used in each iteration of the loop?

A. Inputs

B. Results

C. Input Results

D. Outputs

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

A security analyst is reviewing alerts and incidents associated with internal vulnerability scanning performed by the security operations team. Which built-in incident domain will be assigned to these alerts and incidents in Cortex XSIAM?

A. Security

B. Hunting

C. IT

D. Health

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Why would an analyst schedule an XQL query?

A. To auto-resolve a false positive alert

B. To increase accuracy of queries during off-peak load times

C. To trigger endpoint isolation action

D. To retrieve data either at specific intervals or at a specified time

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!