Question #1 *Topic 1*

How can a customer ingest additional events from a Windows DHCP server into Cortex XDR with minimal configuration?

A. Install the XDR Collector.

B. Enable HTTP collector integration.

C. Activate Windows Event Collector (WEC).

D. Install the Cortex XDR agent.

Suggested Answer: *C*

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

Question #2 *Topic 1*

A query is created that will run weekly via API. After it is tested and ready, it is reviewed in the Query Center.
Which available column should be checked to determine how many compute units will be used when the query is run?

A. Compute Unit Quota

B. Query Status

C. Compute Unit Usage

D. Simulated Compute Units

Suggested Answer: *D*

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

Question #3 *Topic 1*

Some company employees are able to print documents when working from home, but not on network-attached printers, while others are able to print only to file.
What can be inferred about the affected users' inability to print?

A. They may have a host firewall profile set to block activity to all network-attached printers.

B. They may be on different device extensions profiles set to block different print jobs.

C. They may be attached to the default extensions policy and profile.

D. They may have different disk encryption profiles that are not allowing print jobs on encrypted files.

Suggested Answer: *B*

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

Question #4 *Topic 1*

The most recent Cortex XDR agents are being installed at a newly acquired company. A list with endpoint types (i.e., OS, hardware, software) is provided to the engineer.
What should be cross-referenced for the Linux systems listed regarding the OS types and OS versions supported?

A. Kernel Module Version Support

B. Content Compatibility matrix

C. End-of-life summary

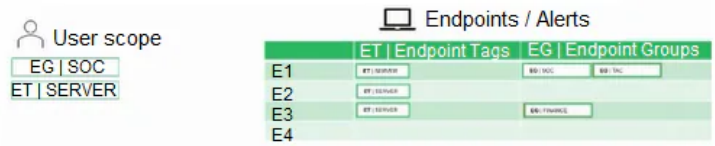
D. Agent Installer Certificate

Suggested Answer: *A*

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

Question #5 *Topic 1*

Based on the SBAC scenario image below, when the tenant is switched to permissive mode, which endpoint(s) data will be accessible?



A. E1 only

B. E2 only

C. E1, E2, and E3

D. E1, E2, E3, and E4

Suggested Answer: *C*

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

Question #6 *Topic 1*

What are two possible actions that can be triggered by a dashboard drilldown? (Choose two.)

A. Initiate automated response actions.

B. Navigate to a different dashboard.

C. Send alerts to console users.

D. Link to an XQL query.

Suggested Answer: *B, D*

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

Question #7 *Topic 1*

An administrator wants to employ reusable rules within custom parsing rules to apply consistent log field extraction across multiple data sources. Which section of the parsing rule should the administrator use to define these reusable rules in Cortex XDR?

A. RULE

B. INGEST

C. FILTER

D. CONST

Suggested Answer: *A*

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

Question #8 *Topic 1*

Which method will drop undesired logs and reduce the amount of data being ingested?

A. [INGEST:vendor= “vendor”, product= “product”, target_dataset= “vendor_product_raw”, no_hit=drop] filter _raw_log not contains “undesired logs”;

B. [COLLECT:vendor= “vendor”, product= “product”, target_dataset=*, no_hit=drop] drop _raw_log contains “undesired logs”;

C. [INGEST:vendor= “vendor”, product= “product”, target_brokers= “vendor_product_raw”, no_hit=keep] filter _raw_log not contains “undesired logs”;

D. [COLLECT:vendor= “vendor”, product= “product”, target_brokers=*, no_hit=drop] drop _raw_log contains “undesired logs”;

Suggested Answer: *B*

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

Question #9 *Topic 1*

A new parsing rule is created, and during testing and verification, all the logs for which field data is to be parsed out are missing. All the other logs from this data source appear as expected.
What may be the cause of this behavior?

A. The XDR Collector is dropping the logs.

B. The filter stage is dropping the logs.

C. The Broker VM is offline.

D. The parsing rule corrupted the database.

Suggested Answer: *B*

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

Question #10 *Topic 1*

What should be configured in Cortex XDR to integrate asset data from Microsoft Azure for better visibility and incident investigation?

A. Cloud Inventory

B. Cloud Identity Engine

C. Microsoft 365

D. Azure Network Watcher

Suggested Answer: *A*

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

Question #11 *Topic 1*

A security audit determines that the Windows Cortex XDR host-based firewall is not blocking outbound RDP connections for certain remote workers. The audit report confirms the following:
All devices are running healthy Cortex XDR agents.
A single host-based firewall rule to block all outbound RDP is implemented.
The policy hosting the profile containing the rule applies to all Windows endpoints.
The logic within the firewall rule is adequate.
Further testing concludes RDP is successfully being blocked on all devices tested at company HQ.
Network location configuration in Agent Settings is enabled on all Windows endpoints.
What is the likely reason the RDP connections are not being blocked?

A. The pertinent host-based firewall rule group is only applied to external rule groups.

B. Report mode is set to Enabled in the report settings under the profile configuration.

C. The pertinent host-based firewall rule group is only applied to internal rule groups.

D. The profile's default action for outbound traffic is set to Allow.

Suggested Answer: *C*

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

Question #12 *Topic 1*

Which XQL query can be saved as a behavioral indicator of compromise (BIOC) rule, then converted to a custom prevention rule?

A.
```
dataset = xdr_data
| filter event_type = ENUM.PROCESS and event_type = ENUM.DEVICE
and action_process_image_name = "**"
and action_process_image_command_line = "-e cmd*"
and action_process_image_command_line != "*cmd.exe -a /c*"
```

B.
```
dataset = xdr_data
| filter event_type = ENUM.DEVICE and
action_process_image_name = "**"
and action_process_image_command_line = "-e cmd*"
and action_process_image_command_line != "*cmd.exe -a /c*"
```

C.
```
dataset = xdr_data
| filter event_type = FILE and (event_sub_type = FILE_CREATE_NEW or
event_sub_type = FILE_WRITE or event_sub_type = FILTER_REMOVE or
event_sub_type = FILE_RENAME ) and agent_hostname = "hostname"
| filter lowercase(action_file_path) in ("/etc/*", "/usr/local/share/
*". "/usr/share/*") and action_file_extension in ("conf", "txt")
| fields action_file_name, action_file_path , action_file_type ,
agent_ip_addresses , agent_hostname, action_file_path
```

D.
```
dataset = xdr_data
| filter event_type = ENUM.PROCESS and action_process_image_name
= "**"
and action_process_image_command_line = "-e cmd*"
and action_process_image_command_line != "*cmd.exe -a /c*"
```

Suggested Answer: *D*

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

Question #13 *Topic 1*

A multinational company with over 300,000 employees has recently deployed Cortex XDR in North America. The solution includes the Identity Threat Detection and Response (ITDR) add-on, and the Cortex team has onboarded the Cloud Identity Engine to the North American tenant. After waiting the required soak period and deploying enough agents to receive identity and threat analytics detections, the team does not see user, group, or computer details for individuals from the European offices.
What may be the reason for the issue?

A. The Cloud Identity Engine plug-in has not been installed and configured.

B. The Cloud Identity Engine needs to be activated in all global regions.

C. The ITDR add-on is not compatible with the Cloud Identity Engine.

D. The XDR tenant is not in the same region as the Cloud Identity Engine.

Suggested Answer: *B*

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

Question #14 *Topic 1*

Using the Cortex XDR console, how can additional network access be allowed from a set of IP addresses to an isolated endpoint?

A. Add entries in the Allowed Domains section of Security Settings for the tenant.

B. Add entries in Configuration section of Security Settings.

C. Add entries in Response Actions section of Agent Settings profile.

D. Add entries in Exceptions Configuration section of Isolation Exceptions.

Suggested Answer: *D*

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

Question #15 *Topic 1*

When isolating Cortex XDR agent components to troubleshoot for compatibility, which command is used to turn off a component on a Windows machine?

A. C:\Program Files\Palo Alto Networks\Traps\cytool.exe stop

B. C:\Program Files\Palo Alto Networks\Traps\xdr.exe runtime stop

C. C:\Program Files\Palo Alto Networks\Traps\cytool.exe runtime stop

D. C:\Program Files\Palo Alto Networks\Traps\xdr.exe stop

Suggested Answer: *C*

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

Question #16 *Topic 1*

During deployment of Cortex XDR for Linux Agents, the security engineering team is asked to implement memory monitoring for agent health monitoring.
Which agent service should be monitored to fulfill this request?

A. pyxd

B. clad

C. pmd

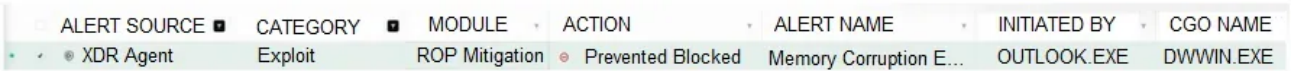
D. dypdng

Suggested Answer: *C*

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

Question #17 *Topic 1*

Based on the image of a validated false positive alert below, which action is recommended for resolution?



ALERT SOURCE	CATEGORY	MODULE	ACTION	ALERT NAME	INITIATED BY	CGO NAME
XDR Agent	Exploit	ROP Mitigation	Prevented Blocked	Memory Corruption E...	OUTLOOK.EXE	DWWIN.EXE

A. Disable injection to the CGO Process DWWIN.EXE.

B. Create an exception for the CGO DWWIN.EXE for ROP Mitigation Module.

C. Create an alert exclusion for OUTLOOK.EXE.

D. Create an exception for OUTLOOK.EXE for ROP Mitigation Module.

Suggested Answer: *D*

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

Question #18 *Topic 1*

What is a benefit of ingesting and forwarding Palo Alto Networks NGFW logs to Cortex XDR?

A. Sending endpoint logs to the NGFW for analysis

B. Automated downloading of malware signatures from the NGFW

C. Enabling additional analysis through enhanced application logging

D. Blocking network traffic based on Cortex XDR detections

Suggested Answer: *C*

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

Question #19 *Topic 1*

How long is data kept in the temporary hot storage cache after being queried from cold storage?

A. 24 hours, re-queried to a maximum of 14 days

B. 24 hours, re-queried to a maximum of 7 days

C. 1 hour, re-queried to a maximum of 12 hours

D. 1 hour, re-queried to a maximum of 24 hours

Suggested Answer: *B*

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

Question #20 *Topic 1*

What will be the output of the function below?
LTRIM("*a* aapple*", "*a")

A. "aapple*"

B. "*aapple*"

C. "pple*"

D. "*aapple"

Suggested Answer: *C*

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

Question #21 *Topic 1*

How can a Malware profile be configured to prevent a specific executable from being uploaded to the cloud?

A. Add the executable to the allow list for executions.

B. Disable on-demand file examination for the executable.

C. Create an exclusion rule for the executable.

D. Set PE and DLL examination for the executable to report action mode.

Suggested Answer: *C*

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

Question #22 *Topic 1*

When onboarding a Palo Alto Networks NGFW to Cortex XDR, what must be done to confirm that logs are being ingested successfully after a device is selected and verified?

A. Conduct an XQL query for NGFW log data.

B. Retrieve device certificate from NGFW dashboard.

C. Confirm that the selected device has a valid certificate.

D. Wait for an incident that involves the NGFW to populate.

Suggested Answer: *A*

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

Question #23 *Topic 1*

Which components may be included in a Cortex XDR content update?

A. Antivirus definitions and agent versions

B. Behavioral Threat Protection (BTP) rules and local analysis logic

C. Device control profiles, agent versions, and kernel support

D. Firewall rules and antivirus definitions

Suggested Answer: *B*

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

Question #24 *Topic 1*

What happens when the XDR Collector is uninstalled from an endpoint by using the Cortex XDR console?

A. The machine status remains active until manually removed, and the configuration data is retained for up to seven days.

B. The files are removed immediately, and the machine is deleted from the system without any retention period.

C. It is uninstalled during the next heartbeat communication, machine status changes to Uninstalled, and the configuration data is retained for 90 days.

D. The associated configuration data is removed from the Action Center immediately after uninstallation.

Suggested Answer: *C*

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

Question #25 *Topic 1*

Which action is being taken with the query below?

```
dataset=xdr_data
| fields agent_hostname, _time, _product
| comp latest (_time) as latest_time by agent_hostname, _product
| join type=inner (dataset=endpoints
    | fields endpoint_name, endpoint_status, endpoint_type) as lookup
lookup.endpoint_name=agent_hostname
| filter endpoin_status = ENUM.CONNECTED
| fields agent_hostname, endpoint_status, latest_time, _product
```

A. Identifying endpoints that have disconnected from the network

B. Checking for endpoints with outdated agent versions

C. Monitoring the latest activity of endpoints

D. Monitoring the latest activity of connected firewall endpoints

Suggested Answer: *C*

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

Question #26 *Topic 1*

Which statement describes the functionality of fixed filters and dashboard drilldowns in enhancing a dashboard's interactivity and data insights?

A. Fixed filters allow users to adjust the layout, while dashboard drilldowns provide links to external reports and/or dashboards.

B. Fixed filters allow users to select predefined data values, while dashboard drilldowns enable users to alter the scope of the data displayed by selecting filter values from the dashboard header.

C. Fixed filters let users select predefined or dynamic values to adjust the scope, while dashboard drilldowns provide interactive insights or trigger contextual changes, like linking to XQL searches.

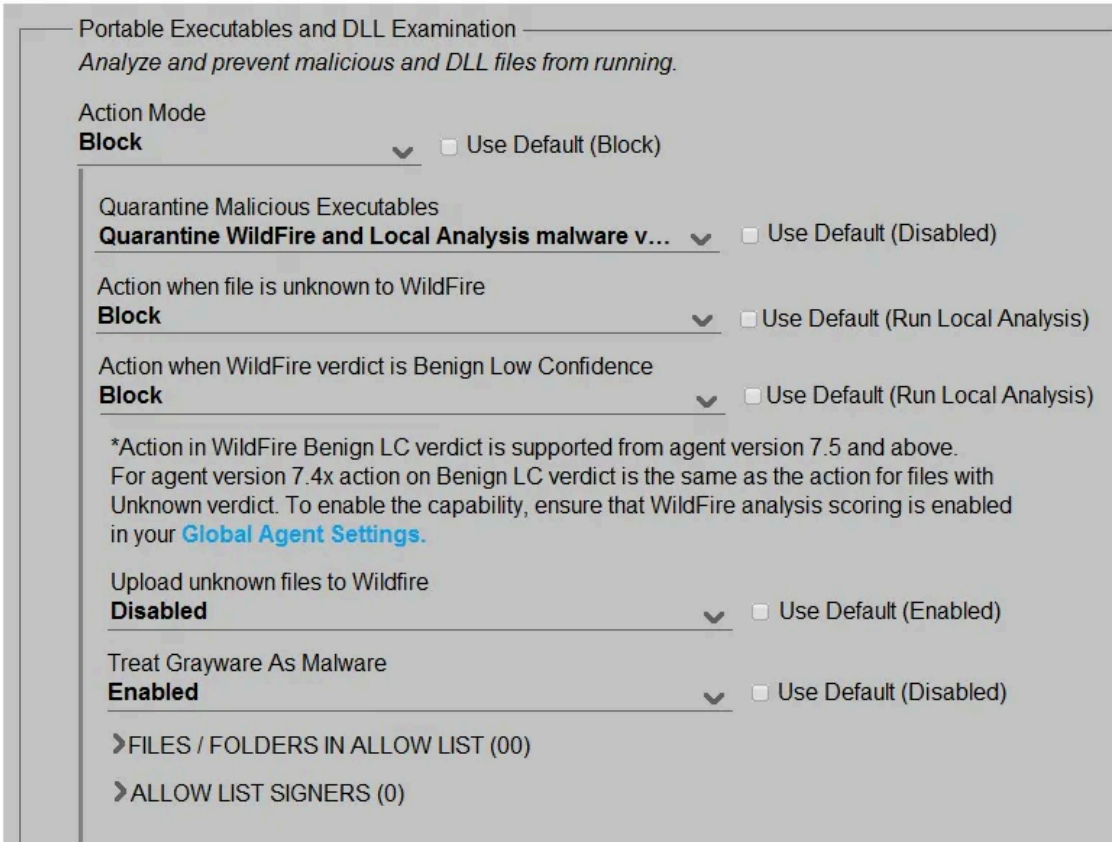
D. Fixed filters limit the data visible in widgets, while dashboard drilldowns allow users to download data from the dashboard in various formats.

Suggested Answer: *C*

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

Question #27 *Topic 1*

Based on the Malware profile image below, what happens when a new custom-developed application attempts to execute on an endpoint?



A. It will execute after one hour.

B. It will immediately execute.

C. It will execute after the second attempt.

D. It will not execute.

Suggested Answer: *D*

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

Question #28 *Topic 1*

Log events from a previously deployed Windows XDR Collector agent are no longer being observed in the console after an OS upgrade.
Which aspect of the log events is the probable cause of this behavior?

A. They are greater than 5MB.

B. They are in Filebeat format.

C. They are in Winlogbeat format.

D. They are less than 1MB.

Suggested Answer: *A*

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

Question #29 *Topic 1*

During the deployment of a Broker VM in a high availability (HA) environment, after configuring the Broker VM FQDN, an XDR engineer must ensure agent installer availability and efficient content caching to maintain performance consistency across failovers.
Which additional configuration steps should the engineer take?

A. Use shared SSL certificates and keys for all Broker VMs and configure a single IP address for failover.

B. Enable synchronized session persistence across Broker VMs and use a self-signed certificate and key.

C. Deploy a load balancer and configure SSL termination at the load balancer.

D. Upload the signed SSL server certificate and key and deploy a load balancer.

Suggested Answer: *D*

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