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

[Data Ingestion and Integration]
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 those reusable rules in Cortex XDR?

A. RULE
B. INGEST
C. FILTER
D. CONST

Answer: D

Question: 2

[Data Ingestion and Integration]
What will be the output of the function below?
L_TRIM("a* aapple", "a")

A. ' aapple'
B. '' aapple"
C. ''pple"
D. '' aapple-"

Answer: A

Question: 3

[Data Ingestion and Integration]
How can a customer ingest additional events from a Windows DHCP server into Cortex XDR with minimal configuration?

A. Activate Windows Event Collector (WEC)
B. Install the XDR Collector
C. Enable HTTP collector integration
D. Install the Cortex XDR agent

Answer: B

Question: 4

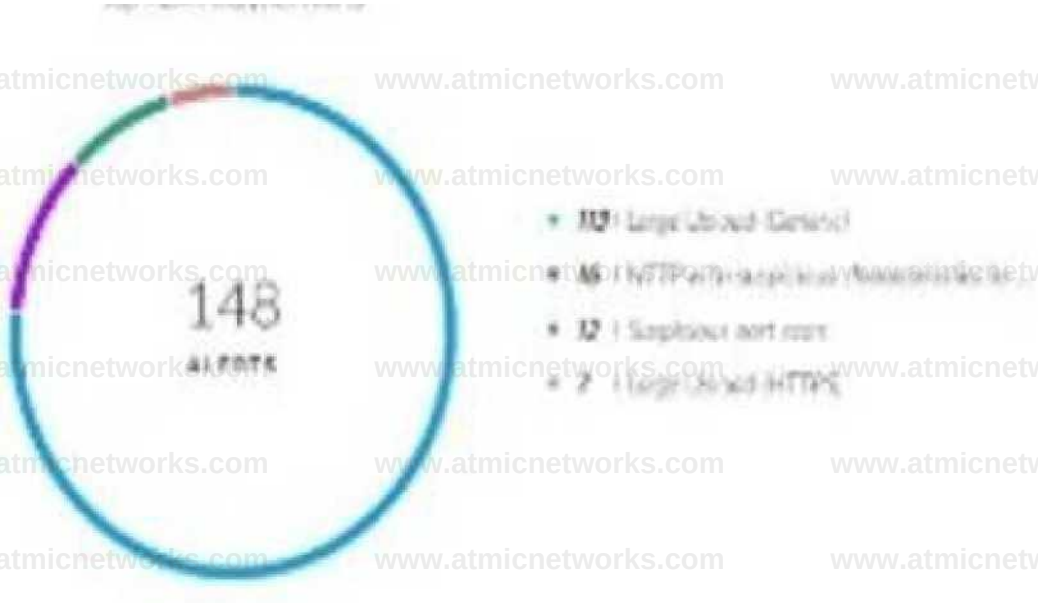
[Cortex XDR Agent Configuration]
How are dynamic endpoint groups created and managed in Cortex XDR?

A. Endpoint groups require intervention to update the group with new endpoints when a new device is added to the network
B. Each endpoint can belong to multiple groups simultaneously, allowing different security policies to be applied to the same device at the same time
C. After an endpoint group is created, its assigned security policy cannot be changed without deleting and recreating the group
D. Endpoint groups are defined based on fields such as OS type, OS version, and network segment

Answer: D

Question: 5

[Dashboards and Reporting]
An engineer is building a dashboard to visualize the number of alerts from various sources. One of the widgets from the dashboard is shown in the image below:



The engineer wants to configure a drilldown on this widget to allow dashboard users to select any of the alert names and view those alerts with additional relevant details. The engineer has configured the following XQL query to meet the requirement:

dataset = alerts

| fields alert_name, description, alert_source, severity, original_tags, alert_id, incident_id
| filter alert_name =
| sort desc _time

How will the engineer complete the third line of the query (filter alert_name =) to allow dynamic filtering on a selected alert name?

A. $y_axis.value
B. $x_axis.value
C. $x_axis.name
D. $y_axis.name

Answer: B

Question: 6

[Detection Engineering]
An XDR engineer is creating a correlation rule to monitor login activity on specific systems. When the activity is identified, an alert is created. The alerts are being generated properly but are missing the username when viewed. How can the username information be included in the alerts?

A. Select “Initial Access” in the MITRE ATT&CK mapping to include the username
B. Update the query in the correlation rule to include the username field
C. Add a mapping for the username field in the alert fields mapping
D. Add a drill-down query to the alert which pulls the username field

Answer: C

Question: 7

[Detection Engineering]
A correlation rule is created to detect potential insider threats by correlating user login events from one dataset with file access events from another dataset. The rule must retain all user login events, even if there are no matching file access events, to ensure no login activity is missed.
text
Copy
dataset = x
| join (dataset = y)

Which type of join is required to maintain all records from dataset x, even if there are no matching events from dataset y?

A. Inner
B. Left
C. Right
D. Outer

Answer: B

Question: 8

[Post-Deployment Management and Configuration]
A cloud administrator reports high network bandwidth costs attributed to Cortex XDR operations and asks for bandwidth usage to be optimized without compromising agent functionality. Which two techniques should the engineer implement? (Choose two.)

A. Configure P2P download sources for agent upgrades and content updates
B. Enable minor content version updates
C. Enable agent content management bandwidth control
D. Deploy a Broker VM and activate the local agent settings applet

Answer: A,C

Question: 9

[Cortex XDR Agent Configuration]

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

A. Disable on-demand file examination for the executable
B. Set PE and DLL examination for the executable to report action mode
C. Add the executable to the allow list for executions
D. Create an exclusion rule for the executable

Answer: D

Question: 10

[Planning and Installation]
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 additionalconfiguration 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. Upload the-signed SSL server certificate and key and deploy a load balancer
C. Deploy a load balancer and configure SSL termination at the load balancer
D. Enable synchronized session persistence across Broker VMs and use a self-signed certificate and key

Answer: B

Question: 11

[Cortex XDR Agent Configuration]

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

A. It will immediately execute
B. It will not execute
C. It will execute after one hour
D. It will execute after the second attempt

Answer: B

Question: 12

[Data Ingestion and Integration]
Which configuration profile option with an available built-in template can be applied to both Windows and Linux systems by using XDR Collector?

A. Filebeat
B. HTTP Collector template
C. XDR Collector settings
D. Winlogbeat

Answer: A

Question: 13

[Detection Engineering]
What is the earliest time frame an alert could be automatically generated once the conditions of a new correlation rule are met?

A. Between 30 and 45 minutes
B. Immediately
C. 5 minutes or less
D. Between 10 and 20 minutes

Answer: C

Question: 14

[Detection Engineering]
A Custom Prevention rule that was determined to be a false positive alert needs to be tuned. The behavior was determined to be authorized and expected on the affected endpoint. Based on the image below, which two steps could be taken? (Choose two.)

[Image description: A Custom Prevention rule configuration, assumed to trigger a Behavioral Indicator of Compromise (BIOC) alert for authorized behavior]

A. Apply an alert exception
B. Apply an alert exclusion to the XDR behavioral indicator of compromise (BIOC) alert
C. Apply an alert exclusion to the XDR agent alert
D. Modify the behavioral indicator of compromise (BIOC) logic

Answer: A,B

Question: 15

[Data Ingestion and Integration]

In addition to using valid authentication credentials, what is required to enable the setup of the Database Collector applet on the Broker VM to ingest database activity?

A. Valid SQL query targeting the desired data
B. Access to the database audit log
C. Database schema exported in the correct format
D. Access to the database transaction log

Answer: A

Question: 16

[Data Ingestion and Integration]
Which step is required to configure a proxy for an XDR Collector?

A. Edit the YAML configuration file with the new proxy information
B. Restart the XDR Collector after configuring the proxy settings
C. Connect the XDR Collector to the Pathfinder
D. Configure the proxy settings on the Cortex XDR tenant

Answer: A

Question: 17

[Maintenance and Troubleshooting]
How long is data kept in the temporary hot storage cache after being queried from cold storage?

A. 1 hour, re-queried to a maximum of 12 hours
B. 24 hours, re-queried to a maximum of 7 days
C. 24 hours, re-queried to a maximum of 14 days
D. 1 hour, re-queried to a maximum of 24 hours

Answer: B

Question: 18

[Post-Deployment Management and Configuration]
Which components may be included in a Cortex XDR content update?

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

B. Behavioral Threat Protection (BTP) rules and local analysis logic
C. Antivirus definitions and agent versions
D. Firewall rules and antivirus definitions

Answer: B

Question: 19

[Maintenance and Troubleshooting]
An insider compromise investigation has been requested to provide evidence of an unauthorized removable drive being mounted on a company laptop. Cortex XDR agent is installed with default prevention agent settings profile and default extension "Device Configuration" profile. Where can an engineer find the evidence?

A. Check Host Inventory -> Mounts
B. dataset = xdr_data | filter event_type = ENUM.MOUNT and event_sub_type = ENUM.MOUNT_DRIVE_MOUNT
C. The requested data requires additional configuration to be captured
D. preset = device_control

Answer: A

Question: 20

[Cortex XDR Agent Configuration]
A static endpoint group is created by adding 321 endpoints using the Upload From File feature.
However, after group creation, the members count field shows 244 endpoints. What are two possible reasons why endpoints were not added to the group? (Choose two.)

A. Static groups have a limit of 250 endpoints when adding by file
B. Endpoints added to the new group were previously added to an existing group
C. Endpoints added to the group were in Disconnected or Connection Lost status when groupmembership was added
D. The IP address, hostname, or alias of the endpoints must match an existing agent that has registered with the tenant

Answer: C,D

Question: 21

[Dashboards and Reporting]
What are two possible actions that can be triggered by a dashboard drilldown? (Choose two.)

A. Navigate to a different dashboard
B. Initiate automated response actions
C. Link to an XQL query
D. Send alerts to console users

Answer: A,C

Question: 22

[Data Ingestion and Integration]
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 XDR tenant is not in the same region as the Cloud Identity Engine
B. The Cloud Identity Engine plug-in has not been installed and configured
C. The Cloud Identity Engine needs to be activated in all global regions
D. The ITDR add-on is not compatible with the Cloud Identity Engine

Answer: A

Question: 23

[Planning and Installation]
When using Kerberos as the authentication method for Pathfinder, which two settings must be validated on the DNS server? (Choose two.)

A. DNS forwarders
B. Reverse DNS zone
C. Reverse DNS records
D. AD DS-integrated zones

Answer: B,C

Question: 24

[Dashboards and Reporting]
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 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
B. Fixed filters limit the data visible in widgets, while dashboard drilldowns allow users to download data from the dashboard in various formats
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 allow users to adjust the layout, while dashboard drilldowns provide links to external reports and/or dashboards

Answer: C

Question: 25

[Playbook Creation and Automation]
An engineer wants to automate the handling of alerts in Cortex XDR and defines several automation rules with different actions to be triggered based on specific alert conditions. Some alerts do not trigger the automation rules as expected. Which statement explains why the automation rules might not apply to certain alerts?

A. They are executed in sequential order, so alerts may not trigger the correct actions if the rules are not configured properly
B. They only apply to new alerts grouped into incidents by the system and only alerts that generateincidents trigger automation actions
C. They can only be triggered by alerts with high severity; alerts with low or informational severity will not trigger the automation rules
D. They can be applied to any alert, but they only work if the alert is manually grouped into an incident by the analyst

Answer: A

Question: 26

[Detection Engineering]
What will enable a custom prevention rule to block specific behavior?

A. A correlation rule added to an Agent Blocking profile
B. A custom behavioral indicator of compromise (BIOC) added to an Exploit profile

C. A custom behavioral indicator of compromise (BIOC) added to a Restriction profile
D. A correlation rule added to a Malware profile

Answer: C

Question: 27

[Maintenance and Troubleshooting]
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. Query Status
B. Compute Unit Usage
C. Simulated Compute Units
D. Compute Unit Quota

Answer: B

Question: 28

[Cortex XDR Agent Configuration]
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 profile's default action for outbound traffic is set to Allow
B. The pertinent host-based firewall rule group is only applied to external rule groups
C. Report mode is set to Enabled in the report settings under the profile configuration
D. The pertinent host-based firewall rule group is only applied to internal rule groups

Answer: D

Question: 29

[Post-Deployment Management and Configuration]
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 Configuration section of Security Settings
B. Add entries in the Allowed Domains section of Security Settings for the tenant
C. Add entries in Exceptions Configuration section of Isolation Exceptions
D. Add entries in Response Actions section of Agent Settings profile

Answer: C

Question: 30

[Data Ingestion and Integration]
Which method will drop undesired logs and reduce the amount of data being ingested?

A. [COLLECT:vendor="vendor", product="product", target_brokers="", no_hit=drop] * drop _raw_log contains "undesired logs";
B. [INGEST:vendor="vendor", product="product", target_dataset="vendor_product_raw",no_hit=drop] * filter _raw_log not contains "undesired logs";
C. [COLLECT:vendor="vendor", product="product", target_dataset="", no_hit=drop] * drop _raw_log contains "undesired logs";
D. [INGEST:vendor="vendor", product="product", target_brokers="vendor_product_raw", no_hit=keep] * filter _raw_log not contains "undesired logs";

Answer: C

Question: 31

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

A. Create an alert exclusion for OUTLOOK.EXE
B. Disable an action to the CGO Process DWWIN.EXE
C. Create an exception for the CGO DWWIN.EXE for ROP Mitigation Module
D. Create an exception for OUTLOOK.EXE for ROP Mitigation Module

Answer: D

Question: 32

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

A. Azure Network Watcher
B. Cloud Identity Engine
C. Cloud Inventory
D. Microsoft 365

Answer: C

Question: 33

[Post-Deployment Management and Configuration]
What happens when the XDR Collector is uninstalled from an endpoint by using the Cortex XDR console?

A. The files are removed immediately, and the machine is deleted from the system without any retention period
B. The machine status remains active until manually removed, and the configuration data is retained for up to seven days
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

Answer: C

Question: 34

[Maintenance and Troubleshooting]

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 Winlogbeat format
C. They are in Filebeat format
D. They are less than 1MB

Answer: A

Question: 35

[Dashboards and Reporting]

Which action is being taken with the query below?

```
dataset = xdr_data
| fields agent_hostname, _time, _product
| comp latest 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 endpoint_status = ENUM.CONNECTED
| fields agent_hostname, endpoint_status, latest_time, _product
```

A. Monitoring the latest activity of endpoints
B. Identifying endpoints that have disconnected from the network
C. Monitoring the latest activity of connected firewall endpoints
D. Checking for endpoints with outdated agent versions

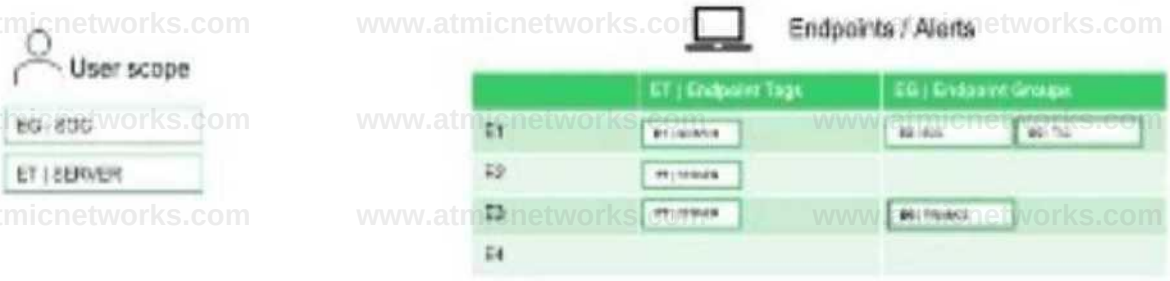
Answer: A

Question: 36

[Post-Deployment Management and Configuration]

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

data will be accessible?

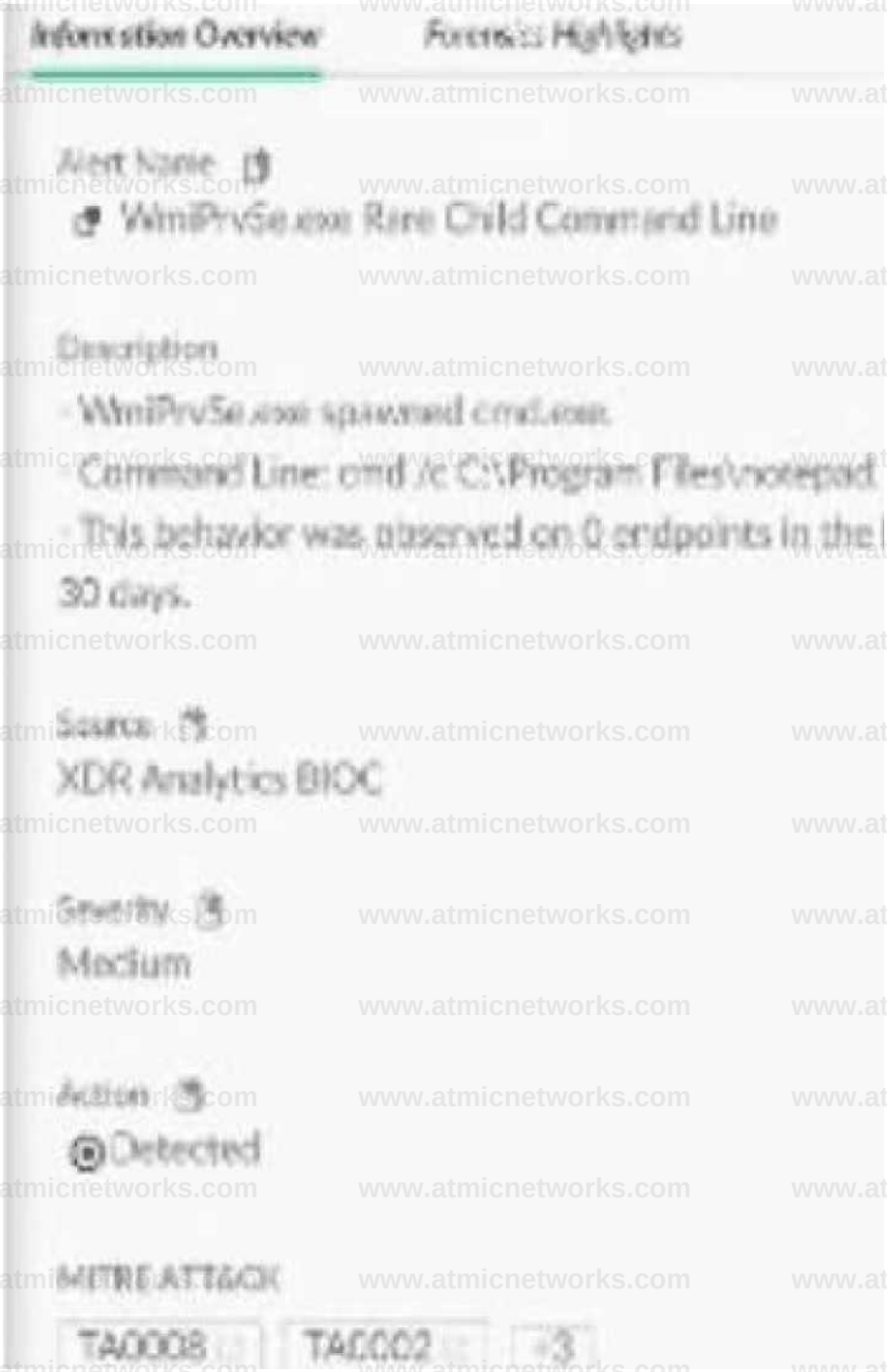


A. E1 only
B. E2 only
C. E1, E2, and E3
D. E1, E2, E3, and E4

Answer: C

Question: 37

[Detection Engineering]
An analyst considers an alert with the category of lateral movement to be allowed and not needing to be checked in the future. Based on the image below, which action can an engineer take to address the requirement?



A. Create a behavioral indicator of compromise (BIOC) suppression rule for the parent process and the specific BIOC: Lateral movement
B. Create an alert exclusion rule by using the alert source and alert name
C. Create a disable injection and prevention rule for the parent process indicated in the alert
D. Create an exception rule for the parent process and the exact command indicated in the alert

Answer: B

Question: 38

[Cortex XDR Agent Configuration]
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 be attached to the default extensions policy and profile
B. They may have a host firewall profile set to block activity to all network-attached printers
C. They may have different disk encryption profiles that are not allowing print jobs on encrypted files D. They may be on different device extensions profiles set to block different print jobs

Answer: B

Question: 39

[Cortex XDR Agent Configuration]
Which two steps should be considered when configuring the Cortex XDR agent for a sensitive and highly regulated environment? (Choose two.)

A. Enable critical environment versions
B. Create an agent settings profile where the agent upgrade scope is maintenance releases only C. Create an agent settings profile, enable content auto-update, and include a delay of four days D. Enable minor content version updates

Answer: B,C

Question: 40

[Maintenance and Troubleshooting]
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\xdr.exe" stop
B. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" runtime stop
C. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" -s stop
D. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" occp

Answer: B

Question: 41

[Planning and Installation]
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. dypdng
B. clad
C. pyxd
D. pmd

Answer: D

Question: 42

[Planning and Installation]
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 crossreferenced for the Linux systems listed regarding the OS types and OS versions supported?

A. Content Compatibility Matrix
B. Kernel Module Version Support
C. End-of-Life Summary
D. Agent Installer Certificate

Answer: B

Question: 43

[Maintenance and Troubleshooting]
After deploying Cortex XDR agents to a large group of endpoints, some of the endpoints have a partially protected status. In which two places can insights into what is contributing to this status be located? (Choose two.)

A. Management Audit Logs
B. XQL query of the endpoints dataset
C. All Endpoints page
D. Asset Inventory

Answer: B,C

Question: 44

[Data Ingestion and Integration]
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. Blocking network traffic based on Cortex XDR detections
C. Enabling additional analysis through enhanced application logging
D. Automated downloading of malware signatures from the NGFW

Answer: C

Question: 45

[Playbook Creation and Automation]
An XDR engineer is configuring an automation playbook to respond to high-severity malware alerts by automatically isolating the affected endpoint and notifying the security team via email. The playbook should only trigger for alerts generated by the Cortex XDR analytics engine, not custom BIOCs. Which two conditions should the engineer include in the playbook trigger to meet these requirements? (Choose two.)

A. Alert severity is High
B. Alert source is Cortex XDR Analytics
C. Alert category is Malware
D. Alert status is New

Answer: A,C

Question: 46

[Data Ingestion and Integration]
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. Wait for an incident that involves the NGFW to populate
C. Confirm that the selected device has a valid certificate
D. Retrieve device certificate from NGFW dashboard

Answer: A

Question: 47

[Detection Engineering]
During a recent internal purple team exercise, the following recommendation is given to the detection engineering team: Detect and prevent command line invocation of Python on Windows endpoints by non-technical business units. Which rule type should be implemented?

A. Analytics Behavioral Indicator of Compromise (ABIOC)
B. Behavioral Indicator of Compromise (BIOC)
C. Correlation
D. Indicator of Compromise (IOC)

Answer: B

Question: 48

[Cortex XDR Agent Configuration]
Multiple remote desktop users complain of in-house applications no longer working. The team uses macOS with Cortex XDR agents version 8.7.0, and the applications were previously allowed by disable prevention rules attached to the Exceptions Profile "Engineer-Mac." Based on the images below, what is a reason for this behavior?

A. Endpoint IP address changed from 192.168.0.0 range to 192.168.100.0 range
B. The Cloud Identity Engine is disconnected or removed
C. XDR agent version was downgraded from 8.7.0 to 8.4.0
D. Installation type changed from VDI to Kubernetes

Answer: A

Question: 49

[Data Ingestion and Integration]
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 Broker VM is ofline
B. The parsing rule corrupted the database
C. The filter stage is dropping the logs
D. The XDR Collector is dropping the logs

Answer: C

Question: 50

[Detection Engineering]
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.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.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*"
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 = FILE_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*"

Answer: D