PaloAltoNetworks.XDR-Engineer.v2026-09-11.q41

Exam Code:	XDR-Engineer
Exam Name:	Palo Alto Networks XDR Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	41
Version:	v2026-09-11
# of views:	105
# of Questions views:	440
https://www.freecram.net/torrent/PaloAltoNetworks.XDR-Engineer.v2026-09-11.q41.html	

NEW QUESTION: 1
What information can be used to create a dynamic endpoint group?
A. Logged-on user
B. MAC address
C. IP address
D. Installed software
Answer: (SHOW ANSWER)
Dynamic endpoint groups can be created using endpoint attributes such as IP address criteria, allowing endpoints to be automatically included when they match the defined network-based condition.

NEW QUESTION: 2
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: (SHOW ANSWER)
In Cortex XDR, Dynamic Endpoint Groups allow you to automatically categorize endpoints based on real-time operational characteristics without manual management.
When you configure a dynamic endpoint group, you establish filtering rules based on specific host attributes. These attributes include OS Type, OS Version, Hostname/String patterns, Domain, and IP address ranges/Network segments. Any endpoint matching these criteria automatically joins the group.

NEW QUESTION: 3
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: (SHOW ANSWER)
On Linux operating systems, the Cortex XDR agent operates through a collection of lightweight background daemons (services).
The Core Daemon: pmd (Protection Management Daemon) is the primary engine service for the Cortex XDR agent on Linux. It is responsible for executing core endpoint security protections, analyzing process activities, managing security policies, and handling local security logic.
Health Monitoring: Because pmd carries out the bulk of the computational heavy lifting for behavioral analysis and log collection, it is the crucial service to track when monitoring memory utilization, CPU consumption, and overall agent health stability.

NEW QUESTION: 4
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: (SHOW ANSWER)
To design a precise trigger condition for an automated response playbook, you must explicitly match the operational parameters requested:
"High-severity malware alerts" $\rightarrow$ A (Alert severity is High)This condition ensures the playbook filters out informational, low, or medium-severity events and only activates when an incident reaches a high risk threshold." Trigger for alerts generated by the Cortex XDR analytics engine, not custom BIOCs"
$\rightarrow$ B (Alert source is Cortex XDR Analytics)The Alert source field specifies which detection engine produced the alert. Restricting the source to Cortex XDR Analytics natively fulfills the requirement by completely isolating machine-learning/anomaly alerts and ignoring events sourced from BIOC or IOC rule engines.

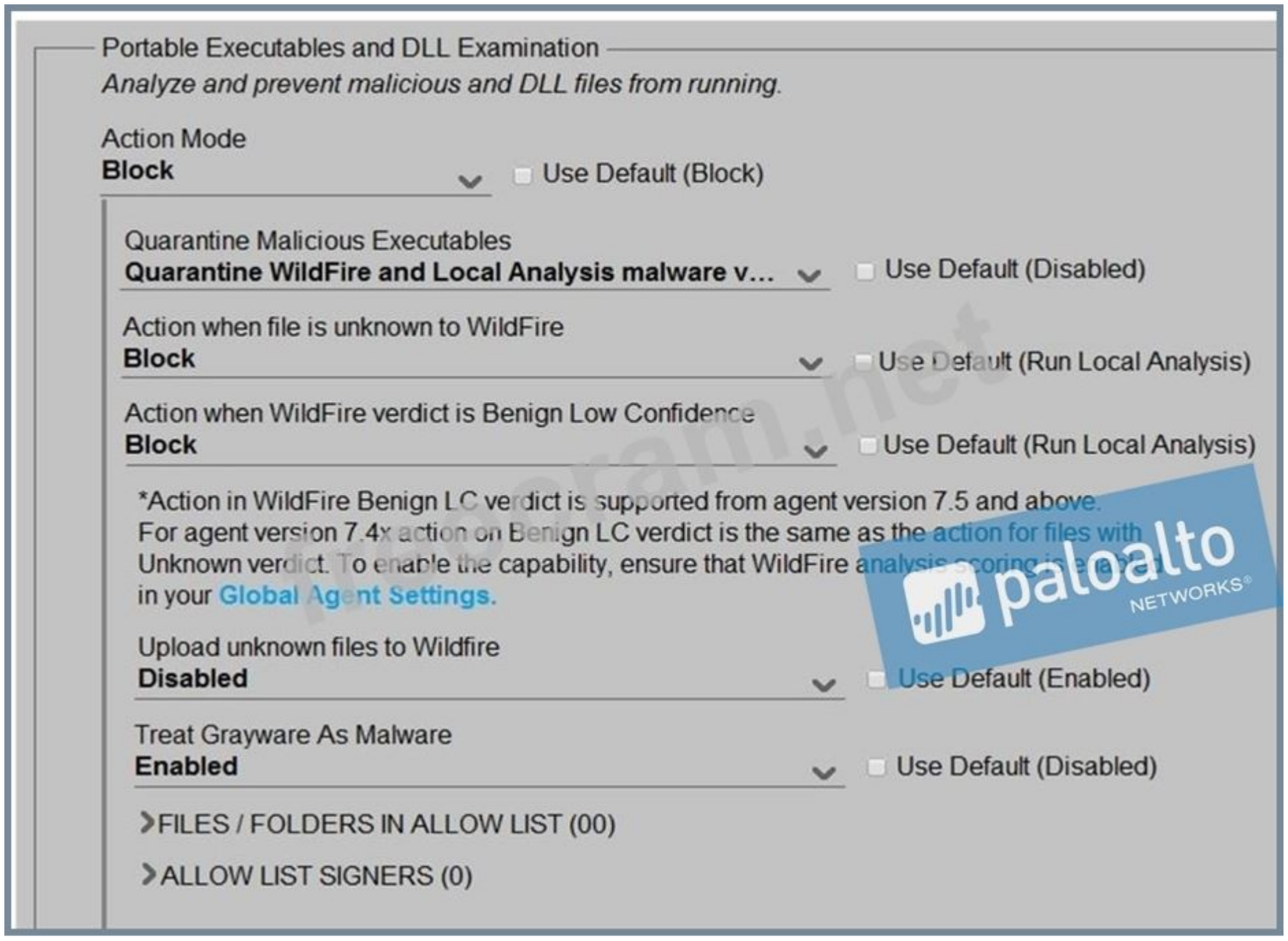
NEW QUESTION: 5
Log events from a previously deployed Windows XDR Collector agent are no longer being observed in the console after an OS upgrade. Which aspect of the log events is the probable cause of this behavior?
A. They are greater than 5MB
B. They are in Winlogbeat format
C. They are in Filebeat format
D. They are less than 1MB
Answer: A (LEAVE A REPLY)
After a Windows OS upgrade, previously configured XDR Collector log sources may begin generating larger log events. Cortex XDR Collector has limitations on the size of events it can process and forward. Events that exceed the supported maximum size (commonly referenced as
5 MB) may be dropped and therefore no longer appear in the Cortex XDR console.

NEW QUESTION: 6
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: (SHOW ANSWER)
In Cortex XDR/XSIAM, querying cold storage datasets consumes Compute Units (CU) based on the timeframe, dataset size, and query complexity. To prevent unnecessary CU consumption and speed up repetitive administrative tasks or consecutive incident lookups, Palo Alto Networks utilizes a caching architecture:
Rewarmed Data Cache: When an XQL query pulls historical data from cold storage, the retrieved logs are "rewarmed" and copied into a temporary hot storage cache.
Duration and Extensions: This rewarmed data remains instantly available in the cache for 24 hours at no additional CU cost. If you or another analyst run a subsequent query covering the same time range within that window, the 24-hour expiration timer resets. This rolling extension can be repeated up to a maximum lifetime of 7 days, after which the cache expires completely, and a brand-new retrieval from cold storage is required.

NEW QUESTION: 7
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: (SHOW ANSWER)
The custom syntax used to write Palo Alto Networks Cortex XDR/XSIAM Parsing Rules (known as XQL for Parsing, or XQLp) breaks a rule file down into distinct, specialized structural blocks:
The RULE Section: This optional section is explicitly designed to define isolated, standalone processing components or logic sequences (such as a specific log field extraction pattern). Because these blocks are tagged with a custom name, they can be repeatedly invoked inside multiple INGEST statements using the call stage syntax (alter field = call ruleName;). This allows you to apply the exact same log parsing logic across completely different log types or data sources without rewriting the code.

NEW QUESTION: 8
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 (LEAVE A REPLY)

Based on the profile settings shown:

Action Mode: Block

Action when file is unknown to WildFire: Block

A new custom-developed application would be unknown to WildFire (no prior verdict exists for it).

With the "Action when file is unknown to WildFire" explicitly set to Block, the file will be prevented from executing.

Additionally, Upload unknown files to WildFire is Disabled, meaning the file won't even be submitted for analysis - it simply gets blocked with no detonation path.

NEW QUESTION: 9
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: (SHOW ANSWER)
When Palo Alto Networks NGFW logs are ingested into Cortex XDR, they provide additional network and application context that enhances XDR's analytics and detection capabilities. The firewall logs can be correlated with endpoint, user, and network activity, enabling enhanced application logging and deeper analysis across the environment.

NEW QUESTION: 10
An analyst uploads custom file hashes associated with a newly discovered threat actor campaign.
What occurs after the IOC is activated?

A. Future activity only is evaluated
B. Historical and future telemetry is analyzed
C. Existing incidents are archived
D. Prevention policies are disabled
Answer: (SHOW ANSWER)
IOC matching evaluates historical telemetry for previous compromises while continuously monitoring future events. This dual capability allows organizations to identify both existing infections and newly emerging threat activity.

NEW QUESTION: 11
A Cortex XDR administrator wants to suppress alerts generated by a trusted internal application without creating unnecessary security blind spots. What is recommended?
A. Disable Behavioral Protection
B. Create Scoped Exceptions
C. Remove Endpoints from Management
D. Disable Incident Correlation
Answer: (SHOW ANSWER)
Scoped exceptions target specific trusted behaviors while preserving overall visibility and protection. Broad exclusions can weaken security controls and create opportunities for attackers to evade detection.

NEW QUESTION: 12
A security analyst is using Cortex XDR to analyze web server logs from an Apache server and wants to build a parsing rule to structure the incoming JSON-formatted logs, with the intent to extract specific fields.
Based on the log image below, which JSON function should be used to extract remote_ip, scanned_ip, and source_log fields?

```
{
“timestamp”: “2022-03-15T10:45:30Z”,
“msg”: “SQL Injection attempt detected”,
“remote_ip”: “192.168.1.101”,
“scanned_ip”: “10.0.0.1”,
“source-log”: “DVWA Security Logs”,
“request”: {
     “method”: “POST”,
     “url”: “/dvwa/vulnerabilities/sqli/”,
     “user_agent”: “Mozilla/5.0 (Windows NT 10.0; Win64; x64
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.0.1
Safari/537.0”
},
“response”: {
“status_code”: 403,
“bytes_sent”: 0
               }
}
```


A. json_extract_string
B. to_json_string
C. json_extract_scalar
D. json_extract_array
Answer: (SHOW ANSWER)
json_extract_scalar is used to extract scalar values such as strings, numbers, or booleans from JSON-formatted log fields. The remote IP, scanned IP, and source log values are scalar fields, so this function is appropriate for parsing them into structured fields.

NEW QUESTION: 13
An organization wants endpoints automatically isolated when high-confidence ransomware activity is detected. Which Cortex XDR capability provides this automation?
A. IOC Expiration Policies
B. Dynamic Host Inventory
C. Response Action Rules
D. Local Analysis Engine
Answer: (SHOW ANSWER)
Response Action Rules automate remediation activities based on predefined criteria. Security teams can automatically isolate devices, collect forensic evidence, or terminate processes when specific threat conditions are satisfied.

NEW QUESTION: 14
A Cortex XDR agent needs to be uninstalled from two Windows machines that are no longer connected to the Cortex XDR tenant.
The uninstall password for the machines is not known.
Which set of actions should be taken to resolve this issue?
A. Run the cytool.exe protect disable command on each machine then uninstall the agent.
B. Boot the machines in safe mode then uninstall the agent.
C. Stop the Cortex XDR services and delete the Cortex XDR folders and registry hives.
D. Copy the original agent MSI installer to each machine then run Msiexec.exe with /x option.

Answer: D (LEAVE A REPLY)
For Windows endpoints that are no longer connected to the tenant and where the uninstall password is unavailable, the supported recovery approach is to use the original Cortex XDR agent MSI package locally and invoke Windows Installer with the uninstall option to remove the agent.

NEW QUESTION: 15
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: (SHOW ANSWER)
When you initiate an uninstallation of an agent or collector from the Cortex XDR management console, the action follows an asynchronous lifecycle:
Next Heartbeat Execution: The cloud management console cannot instantly force changes down to an endpoint. Instead, it creates a pending action. The next time the endpoint checks in with the cloud (its heartbeat communication), it receives the uninstallation command and executes it locally.
Console Status Change: Once the uninstallation is successfully completed and reported back, the endpoint's status in the console updates to Uninstalled.
Data Retention Window: To prevent permanent accidental data loss and to allow administrators time to audit or re-enroll the asset, Cortex XDR retains the machine's configuration data and historic telemetry metadata in the database for a standard buffer period of 90 days before completely purging it.

NEW QUESTION: 16
A Cortex XDR engineer discovers multiple alerts generated across several endpoints. The alerts appear unrelated individually but collectively indicate coordinated malicious activity. What explains this grouping?
A. Endpoint naming convention
B. Dynamic Incident Correlation
C. Asset Inventory Analysis
D. Broker VM Aggregation
Answer: (SHOW ANSWER)
Dynamic Incident Correlation evaluates relationships among alerts, entities, indicators, and attack behaviors. Cortex XDR automatically groups related alerts into incidents, helping analysts understand attack campaigns and reducing investigation time caused by isolated alert review.

NEW QUESTION: 17
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: (SHOW ANSWER)
When configuring Pathfinder (the component used by Cortex XDR/XSIAM to perform host insights and remote analysis on unmanaged or target network endpoints) to use Kerberos for authentication, it relies heavily on proper Active Directory and DNS environmental health.
Kerberos authentication inherently requires mutual authentication and relies on strict name-to-IP and IP-to-name resolution. When Pathfinder attempts to authenticate to an endpoint using Kerberos, it uses the target's IP address to look up its host identity. Therefore, a fully functional Reverse DNS zone containing accurate, up-to-date Reverse DNS records (PTR records) must be validated on the DNS server. If the pointer (PTR) record is missing, incorrect, or doesn't match the forward lookup (A record), Kerberos ticket validation will fail, and authentication will fallback or error out.

NEW QUESTION: 18
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 runtime stop <component>
B. C:\Program Files\Palo Alto Networks\Traps\cytool.exe runtime stop <component>
C. C:\Program Files\Palo Alto Networks\Traps\xdr.exe stop <component>
D. C:\Program Files\Palo Alto Networks\Traps\cytool.exe stop <component>
Answer: (SHOW ANSWER)
When troubleshooting performance or third-party software compatibility issues on an endpoint, administrators use the specialized cytool CLI utility to manage internal agent processes.
The Command Mechanism: Running cytool runtime stop instructs the Cortex XDR agent to temporarily disable or shut down its active real-time protection engines and background services (such as the main supervisor and driver modules).
Security Note: Because the agent is protected against tampering, executing this command from an administrative command prompt typically requires you to first provide the unique uninstallation/protection password generated by the Cortex XDR management console.

NEW QUESTION: 19
A malware profile is configured with all the default settings for a specific endpoint group. For the same group, a restrictions profile has also been configured with the defaults, except with the restriction as shown in the image below. A user opens a command prompt and runs a mimikatz executable from C:\temp.

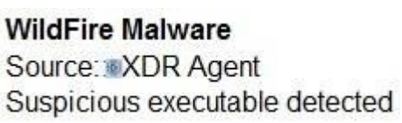
What is the first alert produced on the XDR Console for that endpoint?

A.
Behavioral Threat
Source: XDR Agent
Behavioral threat detected (rule: unit42.mimikatz.33)

B.
Credential Gathering Protection – 657061549
Source: XDR Agent
Mimikatz process_start by name or original file name

C.

D.



Answer: (SHOW ANSWER)

The Restrictions profile blocks executable execution from the configured restricted location. Since the Mimikatz executable is launched from C:\temp and matches the restricted path rule, the first alert generated is for attempted execution from a restricted folder.

NEW QUESTION: 20

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: (SHOW ANSWER)

In Cortex XDR and Cortex XSIAM, Dashboard Drilldowns are designed to provide analysts with interactive pathways to investigate data further when they click on a specific chart element or widget. When configuring a drilldown on a custom widget, the system allows you to define the following target navigation actions:

You can configure the drilldown to open another existing dashboard, passing contextual filters from the clicked item to dynamically alter the scope of the target dashboard.

You can set the click action to pivot the user directly into the XQL Search engine, automatically executing a predefined query pre-populated with variables from the clicked visualization (such as an IP address, host name, or alert type).

NEW QUESTION: 21

What is a limitation of using static endpoint groups in Cortex XDR?

A. Group membership updates are based on real-time threat detection.

B. The selection criteria is limited to 10 and only the *wildcard can be used.

C. Group membership is limited to endpoint tags, partial hostnames and domains, and network information.

D. The endpoint must match an existing XDR agent, with a limit of 250 endpoints.

Answer: (SHOW ANSWER)

Static endpoint groups have limited selection flexibility compared with dynamic groups. Their selection criteria are capped, and wildcard matching is limited to the asterisk character, making them less scalable and adaptive for complex grouping requirements.

NEW QUESTION: 22

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 offline

B. The parsing rule corrupted the database

C. The filter stage is dropping the logs

D. The XDR Collector is dropping the logs

Answer: (SHOW ANSWER)
When configuring custom log ingestion and data modeling in Cortex XDR/XSIAM, Parsing Rules dictate how raw text logs are broken down into specific schema fields (such as IP addresses, timestamps, or usernames).
A parsing rule typically begins with a filter stage (such as a SQL-like filter or regex condition) to isolate and match only the specific log subtypes that need processing out of a broader data stream. If this filter condition is misconfigured, overly restrictive, or contains a typo, the parsing engine will fail to match any incoming records. Instead of parsing them incorrectly, it will drop or exclude those specific logs from the final dataset, while allowing all other unmapped logs from that same vendor source to stream in completely untouched.

NEW QUESTION: 23
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: (SHOW ANSWER)
XDR Collector proxy settings are configured locally by editing the collector's YAML configuration file with the required proxy details. This allows the collector to route its communications through the specified proxy.

NEW QUESTION: 24
An incident is generated from a local analysis malware alert involving install_dependencies.exe.
The hash of the same file now shows a benign verdict from WildFire when viewing the artifacts associated with the incident. Which configuration can be enabled in the Malware profile for this outcome without any additional manual effort from an administrator?
A. "Upload malicious verdicts to WildFire for additional analysis"
B. "Enrich Local Analysis verdicts with WildFire"
C. "Upload unknown files to WildFire"
D. "WildFire Dynamic Re-scan"
Answer: (SHOW ANSWER)
Enriching Local Analysis verdicts with WildFire allows Cortex XDR to automatically use WildFire verdict updates for files initially detected by local analysis. This explains why the incident was generated from a local malware alert, while the artifact hash later shows a benign WildFire verdict without manual administrator action.

NEW QUESTION: 25
An organization experiences recurring malware alerts from the same endpoint despite repeated remediation efforts. What should investigators examine first?
A. Endpoint Screen Resolution
B. Agent Version History
C. Persistence Mechanisms
D. Network Throughput Statistics
Answer: (SHOW ANSWER)
Repeated infections often indicate unresolved persistence methods such as scheduled tasks, services, startup folders, registry run keys, or malicious scripts. Eliminating persistence is essential to preventing reinfection.

NEW QUESTION: 26
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: (SHOW ANSWER)
When a Cortex XDR agent encounters an unknown Portable Executable (PE) or DLL, it can automatically upload the sample to Palo Alto Networks WildFire in the cloud for deep sandboxing and dynamic analysis.
If a specific executable must be prevented from being uploaded to the cloud (for instance, to protect highly confidential corporate proprietary software, proprietary source code compilations, or data privacy requirements), you must configure an Exclusion Rule:
How it works: Under Endpoints > Policy Management > Prevention > Profiles > Malware Profile, you can add a file or path exclusion specifically targeted at WildFire Analysis. By selecting the specific executable or directory and checking the exclusion box for cloud upload/analysis, the local agent will bypass uploading that sample while still enforcing local static analysis protections.

NEW QUESTION: 27
Which agent setting should be enabled when creating the Device Configuration profile to block all network print jobs from all Windows endpoints?
A. Download source P2P settings
B. Windows Security Center integration
C. Agent proxy settings
D. Network location configuration
Answer: (SHOW ANSWER)
Network location configuration is required so Cortex XDR can identify network context and enforce device configuration controls for network-based printing behavior. Enabling it allows the Device Configuration profile to block network print jobs from Windows endpoints.

NEW QUESTION: 28
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: (SHOW ANSWER)
Cortex XDR's Broker VM HA cluster guidance says to use a load balancer FQDN and that, if you use a trusted CA-signed cert, you upload it to the Broker VM; self-signed certs require no extra steps, but HA still relies on the load balancer.

NEW QUESTION: 29
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: (SHOW ANSWER)
When you write a custom correlation rule in Cortex XDR/XSIAM using XQL, the query identifies the matching raw log data. However, simply having the username present in your XQL query results does not automatically mean Cortex knows how to display it in the normalized security alert fields.
During the creation or editing of a correlation rule, there is a dedicated step called Alert Fields Mapping. This section allows you to explicitly map the specific variables or columns generated by your XQL query to standard Cortex XDR alert schema fields (such as actor_user_name, target_user_name, or host_name). If you skip this step, the alert will fire, but critical context like the username will remain blank or unpopulated in the Incident/Alert management console view.

NEW QUESTION: 30
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: (SHOW ANSWER)
XDR Collector supports the deployment of Filebeat on both Windows and Linux systems, and Cortex XDR provides a built-in Filebeat template that can be applied through a configuration profile.

NEW QUESTION: 31
A threat hunter suspects lateral movement activity involving compromised credentials. Which telemetry combination provides the strongest evidence during investigation?
A. Endpoint Naming and Tags
B. Patch Levels and Software Inventory
C. Asset Inventory and Disk Usage
D. Process and Authentication Events
Answer: (SHOW ANSWER)
Combining authentication telemetry with process execution data helps determine whether suspicious activity originated from stolen credentials, malicious processes, or both. This provides critical context for root-cause analysis.

NEW QUESTION: 32
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: (SHOW ANSWER)
By analyzing the alert row columns in the screenshot, we can extract the exact operational data needed to formulate the resolution:
MODULE: ROP Mitigation
INITIATED BY: OUTLOOK.EXE
CGO NAME (Causality Group Owner): DWWIN.EXE (Dr. Watson Windows Error Reporting utility) When an exploit prevention security module trips on a legitimate process (a validated false positive), creating an alert exclusion (triage only) is insufficient because the agent is still actively interrupting the application's functionality. You must configure an exploit exception rule.
In Cortex XDR, exploit protection exceptions must be assigned to the process that initiated the execution chain or was targeted by the exploit technique, rather than the secondary utilities spun up during a crash event (like DWWIN.EXE). Therefore, you create a targeted exploit exception specifying OUTLOOK.EXE as the application process and ROP Mitigation as the specific defense module to bypass.

NEW QUESTION: 33
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: D (LEAVE A REPLY)
The scenario describes two distinct groups with different printing behaviors:
Group 1: can print from home but not to network-attached printers
Group 2: can only print to file
This pattern of differentiated printing restrictions across users is consistent with different device control/extensions profiles being applied, where each profile has different rules blocking specific types of print destinations (network printers vs. all physical printing).

NEW QUESTION: 34
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: (SHOW ANSWER)
All Endpoints page: This is the primary administrative view for agent status in the Cortex XDR console. When an endpoint shows a Partially Protected status, you can hover over the status icon, view the Protection Status column, or open the endpoint's detailed view. This reveals exactly which security modules (such as Malicious Process Execution, Behavioral Threat Protection, or Anti-Exploit) are disabled or failing.

XQL query of the endpoints dataset: For a large group of endpoints, running a Cortex Query Language (XQL) query against the endpoints dataset (e.g., querying fields related to operational status and protection modules) allows you to aggregate, filter, and extract specific granular details on why various endpoints are reporting a partial protection state.

NEW QUESTION: 35
A threat hunter needs to correlate DNS queries, process executions, and network connections across historical telemetry using advanced search logic. Which feature should be used?
A. Asset Inventory
B. Incident Dashboard
C. XQL Search
D. Host Firewall Profiles
Answer: (SHOW ANSWER)
XQL Search allows analysts to query multiple datasets, perform joins, apply aggregations, and build complex hunting workflows. It is specifically designed for advanced investigations requiring deep telemetry correlation across large environments.

NEW QUESTION: 36
Which two Cortex XDR features can be configured to mitigate a potential spike in bandwidth consumption during a Cortex XDR agent upgrade? (Choose two.)
A. Local agent settings with caching enabled on Broker VM
B. Amount of parallel upgrades in the Agent Configurations page
C. Critical environment versions
D. Network location configuration in the agent settings
Answer: (SHOW ANSWER)
Broker VM content caching lets agents download upgrade content locally instead of each endpoint pulling it directly over the WAN, reducing bandwidth impact. Limiting the amount of parallel upgrades controls how many agents upgrade at the same time, preventing a large simultaneous download spike.

NEW QUESTION: 37
An attacker attempts to dump credentials by accessing LSASS memory on a Windows endpoint.
Which Cortex XDR detection capability is most likely involved?
A. Process Behavioral Monitoring
B. Inventory Synchronization
C. Device Profiling
D. Patch Assessment
Answer: (SHOW ANSWER)
Credential dumping techniques often involve abnormal access to sensitive processes such as LSASS. Behavioral monitoring detects suspicious process interactions, privilege escalation attempts, and memory access patterns commonly associated with credential theft.

NEW QUESTION: 38
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: (SHOW ANSWER)

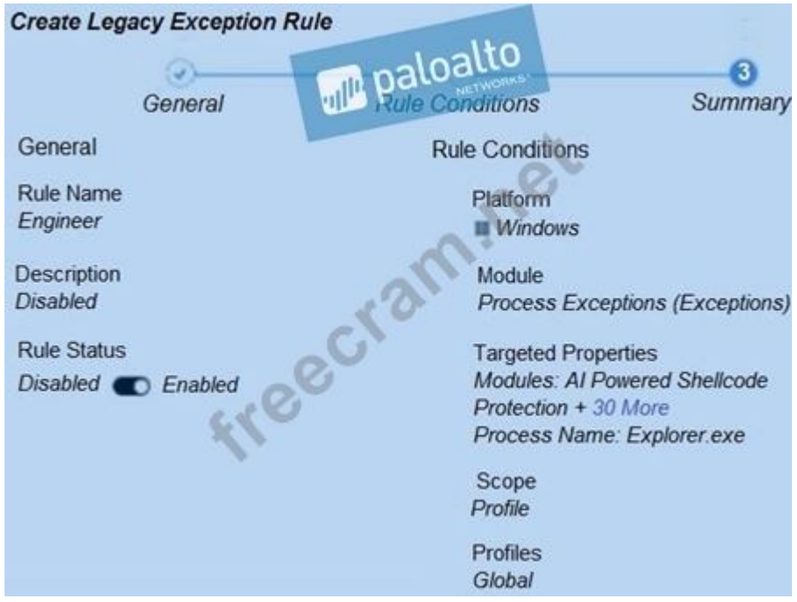
When an endpoint is isolated in Cortex XDR, all network traffic to and from the device is blocked by default, except for traffic explicitly required to communicate with the Cortex XDR management console.
To allow specific, additional administrative or troubleshooting traffic (such as allowing a specific set of IT admin IP addresses to RDP or SSH into the isolated machine), you must configure Isolation Exceptions:
Where to find it: In the Cortex XDR console, you navigate to Settings -> Configurations -> Endpoint Tuning -> Isolation Exceptions.
How it works: Within this section, you define the network rules (IP addresses, ports, and protocols) that the agent should respect even when a "Hard Isolation" or standard isolation command is active on the endpoint.

NEW QUESTION: 39
A mobile device management (MDM) system is configured per documentation, and after Cortex XDR agent deployment, many users show their operational status as "Partially Protected."
What is a potential cause for this behavior?
A. The Safari Safeguard module has not been enabled for all websites.
B. The Network and EDR Security Module is not set to auto-detect malicious URL filtering.
C. Affected users are still using the Default Malware Prevention Module on Policy.
D. URL filtering is currently disabled on the Malware Prevention Module.
Answer: (SHOW ANSWER)
On mobile deployments, the agent can show Partially Protected when the required Safari Safeguard configuration is incomplete. Enabling Safari Safeguard for all websites allows the web protection component to operate fully and changes the device posture from partial protection once the agent reports the updated status.

NEW QUESTION: 40
A threat hunter wants to identify rare parent-child process relationships observed fewer than five times during the previous month. Which approach is most suitable?

A. IOC Matching
B. Incident Review
C. XQL Statistical Analysis
D. Endpoint Isolation
Answer: C (LEAVE A REPLY)
XQL supports aggregations and frequency analysis that help analysts identify uncommon behaviors. Rare process execution chains often indicate attacker activity and are valuable indicators during proactive threat hunting.

NEW QUESTION: 41
Based on the legacy agent exception image below, what is the expected behavior?



A. Once reenabled, Explorer.exe will bypass targeted modules for endpoints by using the Global Exceptions profile.

B. Signed application Explorer.exe from Microsoft will bypass targeted modules for all endpoints.

C. Signed application Explorer.exe from Microsoft will bypass modules for endpoints by using the Global Exceptions profile.

D. Any application named Explorer.exe will bypass targeted modules for endpoints by using the Global Exceptions profile.

Answer: (SHOW ANSWER)

The legacy exception rule targets the process name Explorer.exe without a signer or file path condition. Because the scope is the Global Exceptions profile, any application matching that process name will bypass the targeted prevention modules on endpoints using that profile.