Palo Alto Networks XDR Engineer cexamkiller Praxis Dumps & XDR-Engineer Test Training Überprüfungen

Möchten Sie die nur mit die Hälfte Zeit und Energie bestehen? Dann wählen Sie ExamFragen. Nach mehrjährigen Bemühungen ist die Bestehensquote von der Webseite ExamFragen in der ganzen Welt am höchsten. Wenn Sie die Genauigkeit der Fragenkataloge zur Palo Alto Networks XDR-Engineer Zertifizierungsprüfung aus ExamFragen prüfen möchten, können Sie ein paar Exam Fragen auf der Webseite ExamFragen herunterladen, damit bastätigen Sie Ihre Wahl.

Palo Alto Networks XDR-Engineer Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Detection and Reporting: This section of the exam measures skills of the detection engineer and covers creating detection rules to meet security requirements, including correlation, custom prevention rules, and the use of behavioral indicators of compromise (BIOCs) and indicators of compromise (IOCs). It also assesses configuring exceptions and exclusions, as well as building custom dashboards and reporting templates for effective threat detection and reporting.
Thema 2	• Maintenance and Troubleshooting: This section of the exam measures skills of the XDR engineer and covers managing software component updates for Cortex XDR, such as content, agents, Collectors, and Broker VM. It also includes troubleshooting data management issues like data ingestion and parsing, as well as resolving issues with Cortex XDR components to ensure ongoing system reliability and performance.
Thema 3	• Ingestion and Automation: This section of the exam measures skills of the security engineer and covers onboarding various data sources including NGFW, network, cloud, and identity systems. It also includes managing simple automation rules, configuring Broker VM applets and clusters, setting up XDR Collectors, and creating parsing rules for data normalization and automation within the Cortex XDR environment.
Thema 4	• Planning and Installation: This section of the exam measures skills of the security engineer and covers the deployment process, objectives, and required resources such as hardware, software, data sources, and integrations for Cortex XDR. It also includes understanding and explaining the deployment and functionality of components like the XDR agent, Broker VM, XDR Collector, and Cloud Identity Engine. Additionally, it assesses the ability to configure user roles, permissions, and access controls, as well as knowledge of data retention and compute unit considerations.
Thema 5	• Cortex XDR Agent Configuration: This section of the exam measures skills of the XDR engineer and covers configuring endpoint prevention profiles and policies, setting up endpoint extension profiles, and managing endpoint groups. The focus is on ensuring endpoints are properly protected and policies are consistently applied across the organization.

>> XDR-Engineer Fragenpool <<

XDR-Engineer Übungsmaterialien & XDR-Engineer Lernführung: Palo Alto Networks XDR Engineer & XDR-Engineer Lernguide

Damit Sie ExamFragen sicher wählen, wird nur Teil der online optimalen Palo Alto Networks XDR-Engineer Zertifizierungsprüfungsmaterialien zur Verfügung gestellt. So können Sie sie kostenlos als Probe herunterladen und die Zuverlässigkeit unserer Produkte testen. Wir helfen Ihnen nicht nur, die Prüfung zum ersten Mal zu bestehen, sondern Ihnen auch viel Zeit und Energie zu ersparen. ExamFragen stehen Ihnen die echten und originalen Prüfungsfragen und Antworten zur Verfügung, damit Sie die Palo Alto Networks XDR-Engineer Prüfung 100% bestehen können. Mit Palo Alto Networks XDR-Engineer Zertifikat werden Sie in der IT-Branche leichter befördert. Und Ihre Zukunft werden immer schöner sein.

Palo Alto Networks XDR Engineer XDR-Engineer Prüfungsfragen mit Lösungen (Q37-Q42):

37. Frage
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. Deploy a load balancer and configure SSL termination at the load balancer
- B. Enable synchronized session persistence across Broker VMs and use a self-signed certificate and key
- C. Upload the-signed SSL server certificate and key and deploy a load balancer
- D. Use shared SSL certificates and keys for all Broker VMs and configure a single IP address for failover

Antwort: C

Begründung:
In a high availability (HA) environment, theBroker VMin Cortex XDR acts as a local proxy to facilitate agent communications, content caching, and installer distribution, reducing dependency on direct cloud connections. To ensureagent installer availabilityandefficient content cachingacross failovers, the Broker VM must be configured to handle agent requests consistently, even if one VM fails. This requires proper SSL certificate management and load balancing to distribute traffic across multiple Broker VMs.
* Correct Answer Analysis (B):The engineer shouldupload the signed SSL server certificate and key to each Broker VM to secure communications and ensure trust between agents and the Broker VMs.
Additionally, deploying aload balancerin front of the Broker VMs allows traffic to be distributed across multiple VMs, ensuring availability and performance consistency during failovers. The load balancer uses the configured Broker VM FQDN to route agent requests, and the signed SSL certificate ensures secure, uninterrupted communication. This setup supports content caching and installer distribution by maintaining a stable connection point for agents.
* Why not the other options?
* A. Use shared SSL certificates and keys for all Broker VMs and configure a single IP address for failover: While shared SSL certificates can be used, configuring a single IP address for failover (e.g., via VRRP or a floating IP) is less flexible than a load balancer and may not efficiently handle content caching or installer distribution across multiple VMs. Load balancers are preferred for HA setups in Cortex XDR.
* C. Deploy a load balancer and configure SSL termination at the load balancer: SSL termination at the load balancer means the load balancer decrypts traffic before forwarding it to the Broker VMs, requiring unencrypted communication between the load balancer and VMs. This is not recommended for Cortex XDR, as Broker VMs require end-to-end SSL encryption for security, and SSL termination complicates certificate management.
* D. Enable synchronized session persistence across Broker VMs and use a self-signed certificate and key: Self-signed certificates are not recommended for production HA environments, as they can cause trust issues with agents and require manual configuration. Synchronized session persistence is not a standard feature for Broker VMs and is unnecessary for content caching or installer availability.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes Broker VM HA configuration: "For high availability, deploy multiple Broker VMs behind a load balancer and upload a signed SSL server certificate and key to each VM to secure agent communications" (paraphrased from the Broker VM Deployment section). TheEDU-
260: Cortex XDR Prevention and Deploymentcourse covers Broker VM setup, stating that "a load balancer with signed SSL certificates ensures agent installer availability and content caching in HA environments" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes
"planning and installation" as a key exam topic, encompassing Broker VM deployment for HA.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR

Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer
Datasheet:https://www.paloaltonetworks.com/services/education
/certification#xdr-engineer

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

Antwort: A

Begründung:
In Cortex XDR,correlation rulesare used to detect specific patterns or behaviors (e.g., login activity) by analyzing ingested data and generating alerts when conditions are met. For an alert to include specific fields likeusername, the field must be explicitly mapped in thealert fields mappingconfiguration of the correlation rule. This mapping determines which fields from theunderlying dataset are included in the generated alert's details.
In this scenario, the correlation rule is correctly generating alerts for login activity, but theusernamefield is missing. This indicates that the correlation rule's query may be identifying the relevant events, but the usernamefield is not included in the alert's output fields. To resolve this, the engineer must update thealert fields mappingin the correlation rule to explicitly include theusernamefield, ensuring it appears in the alert details when viewed.
* Correct Answer Analysis (C):Adding a mapping for theusernamefield in thealert fields mapping ensures that the field is extracted from the dataset and included in the alert's metadata. This is done in the correlation rule configuration, where administrators can specify which fields to include in the alert output.
* Why not the other options?
* A. Select "Initial Access" in the MITRE ATT&CK mapping to include the username:
Mapping to a MITRE ATT&CK technique like "Initial Access" defines the type of attack or behavior, not specific fields likeusername. This does not address the missing field issue.
* B. Update the query in the correlation rule to include the username field: While the correlation rule's query must reference theusernamefield to detect relevant events, including it in the query alone does not ensure it appears in the alert's output. Thealert fields mappingis still required.
* D. Add a drill-down query to the alert which pulls the username field: Drill-down queries are used for additional investigation after an alert is generated, not for including fields in the alert itself. This does not solve the issue of missingusernamein the alert details.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes correlation rule configuration: "To include specific fields in generated alerts, configure the alert fields mapping in the correlation rule to map dataset fields, such as username, to the alert output" (paraphrased from the Correlation Rules section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers detection engineering, stating that "alert fields mapping determines which data fields are included in alerts generated by correlation rules" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing correlation rule configuration.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR Investigation and Response Course Objectives Palo Alto Networks Certified XDR Engineer
Datasheet:https://www.paloaltonetworks.com/services/education
/certification#xdr-engineer

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

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

Antwort: B,C

Begründung:
In Cortex XDR,dashboard drilldownsallow users to interact with widgets (e.g., charts or tables) by clicking on elements to access additional details or perform actions. Drilldowns enhance the investigative capabilities of dashboards by linking to related data or views.
* Correct Answer Analysis (A, C):
* A. Navigate to a different dashboard: A drilldown can be configured to navigate to another dashboard, providing a more detailed view or related metrics. For example, clicking on an alert count in a widget might open a dashboard focused on alert details.
* C. Link to an XQL query: Drilldowns often link to anXQL querythat filters data based on the clicked element (e.g., an alert name or source). This allows users to view raw events or detailed records in the Query Builder or Investigation view.
* Why not the other options?
* B. Initiate automated response actions: Drilldowns are primarily for navigation and data exploration, not for triggering automated response actions. Response actions (e.g., isolating an endpoint) are typically initiated from the Incident or Alert views, not dashboards.
* D. Send alerts to console users: Drilldowns do not send alerts to users. Alerts are generated by correlation rules or BIOCs, and dashboards are used for visualization, not alert distribution.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes drilldown functionality: "Dashboard drilldowns can navigate to another dashboard or link to an XQL query to display detailed data based on the selected widget element" (paraphrased from the Dashboards and Widgets section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers dashboards, stating that "drilldowns enable navigation to other dashboards or XQL queries for deeper analysis" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "dashboards and reporting" as a key exam topic, encompassing drilldown configuration.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR Investigation and Response Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

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

Antwort: B,C

Begründung:
In Cortex XDR, apartially protected statusfor an endpoint indicates that some agent components or protection modules (e.g., malware protection, exploit prevention) are not fully operational, possibly due to compatibility issues, missing prerequisites, or configuration errors. To troubleshoot this status, engineers need to identify the specific components or issues affecting the endpoint, which can be done by examining detailed endpoint data and status information.
* Correct Answer Analysis (B, C):
* B. XQL query of the endpoints dataset: AnXQL (XDR Query Language)query against the endpoints dataset (e.g., dataset = endpoints | filter endpoint_status = "PARTIALLY_PROTECTED" | fields endpoint_name, protection_status_details) provides detailed insights into the reasons for the partially protected status. The endpoints dataset includes fields like protection_status_details, which specify which modules are not functioning and why.
* C. All Endpoints page: TheAll Endpoints pagein the Cortex XDR console displays a list of all endpoints with their statuses, including those that are partially protected. Clicking into an endpoint's details reveals specific information about the protection status, such as which modules are disabled or encountering issues, helping identify the cause of the status.
* Why not the other options?
* A. Management Audit Logs: Management Audit Logs track administrative actions (e.g., policy changes, agent installations), but they do not provide detailed insights into the endpoint's protection status or the reasons for partial protection.
* D. Asset Inventory: Asset Inventory provides an overview of assets (e.g., hardware, software) but does not specifically detail the protection status of Cortex XDR agents or the reasons for partial protection.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains troubleshooting partially protected endpoints:"Use the All Endpoints page to view

detailed protection status, and run an XQL query against the endpoints dataset to identify specific issues contributing to a partially protected status" (paraphrased from the Endpoint Management section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers endpoint troubleshooting, stating that "the All Endpoints page and XQL queries of the endpoints dataset provide insights into partial protection issues" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing endpoint status investigation.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

41. Frage
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_brokers="", no_hit=drop] * drop _raw_log 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";

Antwort: C

Begründung:
In Cortex XDR, managing data ingestion involves defining rules to collect, filter, or drop logs to optimize storage and processing. The goal is todrop undesired logsto reduce the amount of data ingested. The syntax used in the options appears to be a combination of ingestion rule metadata (e.g., [COLLECT] or [INGEST]) and filtering logic, likely written in a simplified query language for log processing. Thedropaction explicitly discards logs matching a condition, whilefilterwithnot containscan achieve similar results by keeping only logs that do not match the condition.
* Correct Answer Analysis (C):The method in option C,[COLLECT:vendor="vendor", product=" product", target_dataset="", no_hit=drop] * drop _raw_log contains "undesired logs";, explicitly dropslogs where the raw log content contains "undesired logs". The [COLLECT] directive defines the log collection scope (vendor, product, and dataset), and the no_hit=drop parameter indicates that unmatched logs are dropped. The drop _raw_log contains "undesired logs" statement ensures that logs matching the "undesired logs" pattern are discarded, effectively reducing the amount of data ingested.
* Why not the other options?
* A. [COLLECT:vendor="vendor", product="product", target_brokers="", no_hit=drop] * drop _raw_log contains "undesired logs";: This is similar to option C but uses target_brokers="", which is typically used for Broker VM configurations rather than direct dataset ingestion. While it could work, option C is more straightforward with target_dataset="".
* B. [INGEST:vendor="vendor", product="product", target_dataset="vendor_product_raw", no_hit=drop] * filter _raw_log not contains "undesired logs";: This method uses filter _raw_log not contains "undesired logs" to keep logs that do not match the condition, which indirectly drops undesired logs. However, the drop action in option C is more explicit and efficient for reducing ingestion.
* D. [INGEST:vendor="vendor", product="product", target_brokers="vendor_product_raw", no_hit=keep] * filter _raw_log not contains "undesired logs";: The no_hit=keep parameter means unmatched logs are kept, which does not align with the goal of reducing data. The filter statement reduces data, but no_hit=keep may counteract this by retaining unmatched logs, making this less effective than option C.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains log ingestion rules: "To reduce data ingestion, use the drop action to discard logs matching specific patterns, such as _raw_log contains 'pattern'" (paraphrased from the Data Ingestion section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers data ingestion optimization, stating that "dropping logs with specific content using drop _raw_log contains is an effective way to reduce ingested data volume" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing log filtering and dropping.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

42. Frage

.....

Mit ExamFragen können Sie sich nicht nur wertvolle Zeit ersparen, sondern auch sich ganz beruhigt auf die Prüfung vorbereiten und sie erfolgreich bestehen. ExamFragen hat eine gute Zuverlässigkeit und ein hohes Ansehen in der IT-Branche. Sie können kostenlos einen Teil der von ExamFragen gebotene Palo Alto Networks XDR-Engineer Prüfungsfragen und Antworten als Probe herunterladen, um die Zuverlässigkeit unserer Produkte zu testen. Sie werden sicher mit unserern Produkten sehr zufrieden sein. Ich habe Vertrauen in unsere Produkte und glaube, dass die von ExamFragen bietenden Prüfungsfragen und Antworten zu Palo Alto Networks XDR-Engineer Zertifizierung bald Ihre beste Wahl sein würden. Und sie würden sicher die XDR-Engineer Zertifizierungsprüfung erfolgreich abschließen. Es ist ratsam, ExamFragen zu wählen. ExamFragen würde Ihnen die zufriedenen Produkte bieten.

XDR-Engineer Deutsch Prüfung: https://www.examfragen.de/XDR-Engineer-pruefung-fragen.html