XDR-Engineer技術問題、XDR-Engineer復習テキスト

ちなみに、JPTestKing XDR-Engineerの一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1-1maPyEtXbj2e98577oX_9aigccuMTYK

合格できるPalo Alto Networks Palo Alto Networks XDR Engineer試験はいくつありますか？ それらをすべて試してみてください！ JPTestKingは、Palo Alto Networks XDR Engineer コーススペシャリストが開発した実際のPalo Alto Networks XDR-Engineerの回答を含むPalo Alto Networks XDR Engineer XDR-Engineer試験問題への完全なアクセス権をUnlimited Access Planに提示します。 Palo Alto Networks Palo Alto Networks XDR Engineerテストに合格できるだけでなく、さらに良くなります！ また、すべての試験の質問と回答にアクセスして、合計1800以上の試験に合格することもできます。

Palo Alto Networks XDR-Engineer 認定試験の出題範囲：

トピック	出題範囲
トピック 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.
トピック 2	- 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.
トピック 3	- 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.
トピック 4	- 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.
トピック 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.

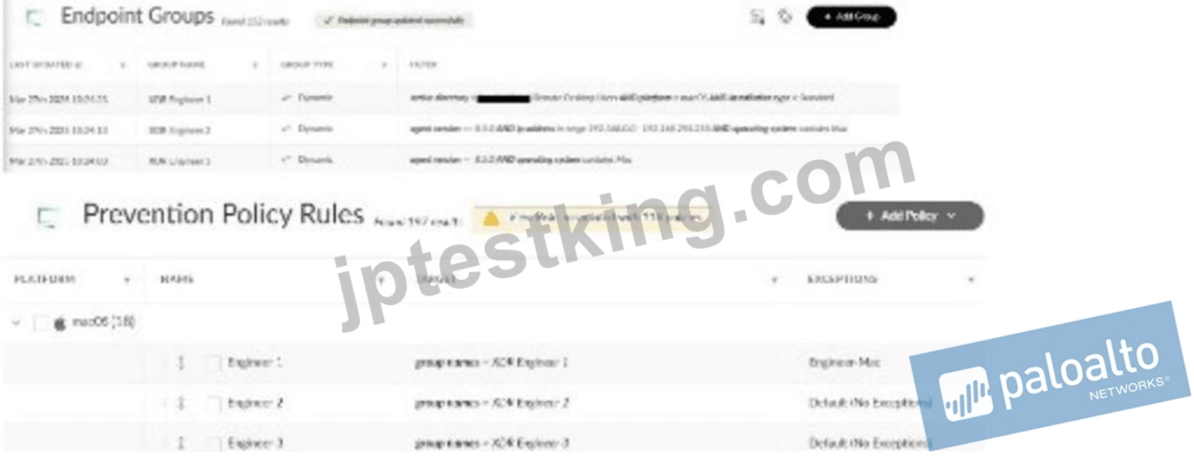
>> XDR-Engineer技術問題 <<

XDR-Engineer復習テキスト & XDR-Engineer日本語版参考書

XDR-Engineer試験の質問は、当社の製品を使用して試験を準備し、夢の証明書を取得できると信じています。より良い求人を希望する場合は、適切なプロ品質を備えなければならないことを私たちは皆知っています。私たちのXDR-Engineer学習教材はあなたのそばにいて気配りのあるサービスを提供する用意があります、そして私たちのXDR-Engineer学習教材はすべてのお客様に心からお勧めします。想像できる。 XDR-Engineerトレーニングガイドには多くの利点があります。

Palo Alto Networks XDR Engineer 認定 XDR-Engineer 試験問題 (Q43-Q48):

質問 # 43
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?



Endpoint Groups

LAST UPDATED AT	GROUP NAME	GROUP TYPE	FILTER
[illegible]	XDR Engineer 1	Dynamic	[illegible] [redacted] [illegible]
[illegible]	XDR Engineer 2	Dynamic	[illegible]
[illegible]	[illegible]	Dynamic	[illegible]

Prevention Policy Rules

PLATFORM	NAME	[illegible]	EXCEPTIONS
macOS (18)			
	Engineer 1	group names = XDR Engineer 1	Engineer-Mac
	Engineer 2	group names = XDR Engineer 2	Default (No Exceptions)
	Engineer 3	group names = XDR Engineer 3	Default (No Exceptions)

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

正解：C

解説：
The scenario involves macOS users with Cortex XDR agents (version 8.7.0) who can no longer run in-house applications that were previously allowed via disable prevention rules in the"Engineer-Mac" Exceptions Profile. This profile is applied to an endpoint group (e.g., "Mac-Engineers"). Theissue likely stems from a change in the endpoint group's configuration or the endpoints' attributes, affecting policy application.
* Correct Answer Analysis (A):The reason for the behavior is that theendpoint IP address changed from 192.168.0.0 range to 192.168.100.0 range. In Cortex XDR, endpoint groups can be defined using dynamic criteria, such as IP address ranges, to apply specific policies like the "Engineer-Mac" Exceptions Profile. If the group "Mac-Engineers" was defined to include endpoints in the 192.168.0.0 range, and the remote desktop users' IP addresses changed to the 192.168.100.0 range (e.g., due to a network change or VPN reconfiguration), these endpoints would no longer belong to the "Mac- Engineers" group. As a result, the "Engineer-Mac" Exceptions Profile, which allowed the in-house applications, would no longer apply, causing the applications to be blocked by default prevention rules.
* Why not the other options?
* B. The Cloud Identity Engine is disconnected or removed: The Cloud Identity Engine provides user and group data for identity-based policies, but it is not directly related to Exceptions Profiles or application execution rules. Its disconnection would not affect the application of the "Engineer-Mac" profile.
* C. XDR agent version was downgraded from 8.7.0 to 8.4.0: The question states the users are using version 8.7.0, and there's no indication of a downgrade. Even if a downgrade occurred, it's unlikely to affect the application of an Exceptions Profile unless specific features were removed, which is not indicated.
* D. Installation type changed from VDI to Kubernetes: The installation type (e.g., VDI for virtual desktops or Kubernetes for

containerized environments) is unrelated to macOS endpoints running remote desktop sessions. This change would not impact the application of the Exceptions Profile.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains endpoint group policies: "Dynamic endpoint groups based on IP address ranges apply policies like Exceptions Profiles; if an endpoint's IP changes to a different range, it may no longer belong to the group, affecting policy enforcement" (paraphrased from the Endpoint Management section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers policy application, stating that "changes in IP address ranges can cause endpoints to fall out of a group, leading to unexpected policy behavior like blocking previously allowed applications" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing endpoint group and policy management.
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

質問 # 44
Which method will drop undesired logs and reduce the amount of data being ingested?

- A. [INGEST:vendor="vendor", product="product", target_brokers="vendor_product_raw", no_hit=keep] * 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_dataset="vendor_product_raw",no_hit=drop] * filter _raw_log not contains "undesired logs";

正解：C

解説：
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

質問 # 45
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 can only be triggered by alerts with high severity; alerts with low or informational severity will not trigger the automation rules
- B. They only apply to new alerts grouped into incidents by the system and only alerts that generateincidents trigger automation actions
- C. They are executed in sequential order, so alerts may not trigger the correct actions if the rules are not configured properly
- D. They can be applied to any alert, but they only work if the alert is manually grouped into an incident by the analyst

正解：C

解説：
In Cortex XDR,automation rules(also known as response actions or playbooks) are used to automate alert handling based on specific conditions, such as alert type, severity, or source. These rules are executed in a defined order, and the first rule that matches an alert's conditions triggers its associated actions. If automation rules are not triggering as expected, the issue often lies in their configuration or execution order.
* Correct Answer Analysis (A):Automation rules areexecuted in sequential order, and each alert is evaluated against the rules in the order they are defined. If the rules are not configured properly (e.g., overly broad conditions in an earlier rule or incorrect prioritization), an alert may match an earlier rule and trigger its actions instead of the intended rule, or it may not match any rule due to misconfigured conditions. This explains why some alerts do not trigger the expected automation rules.
* Why not the other options?
* B. They only apply to new alerts grouped into incidents by the system and only alerts that generate incidents trigger automation actions: Automation rules can apply to both standalone alerts and those grouped into incidents. They are not limited to incident-related alerts.
* C. They can only be triggered by alerts with high severity; alerts with low or informational severity will not trigger the automation rules: Automation rules can be configured to trigger based on any severity level (high, medium, low, or informational), so this is not a restriction.
* D. They can be applied to any alert, but they only work if the alert is manually grouped into an incident by the analyst: Automation rules do not require manual incident grouping; they can apply to any alert based on defined conditions, regardless of incident status.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains automation rules: "Automation rules are executed in sequential order, and the first rule matching an alert's conditions triggers its actions. Misconfigured rules or incorrect ordering can prevent expected actions from being applied" (paraphrased from the Automation Rules section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers automation, stating that
"sequential execution of automation rules requires careful configuration to ensure the correct actions are triggered" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheet includes "playbook creation and automation" as a key exam topic, encompassing automation 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

質問 # 46
What will enable a custom prevention rule to block specific behavior?

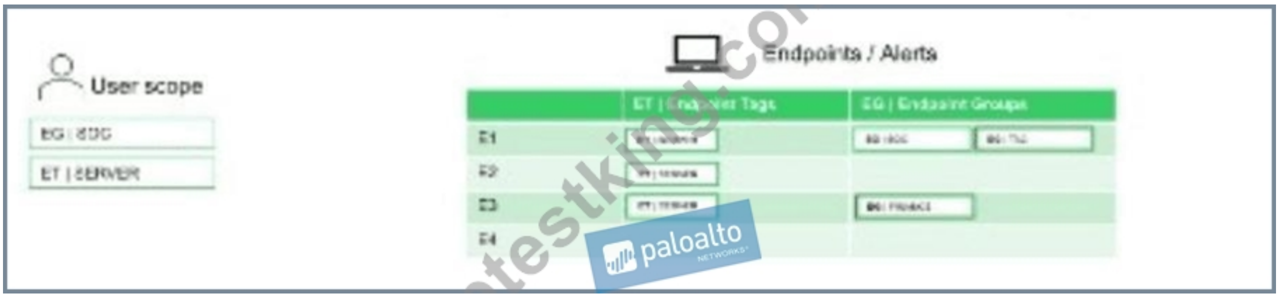
- A. A custom behavioral indicator of compromise (BIOC) added to an Exploit profile
- B. A correlation rule added to a Malware profile
- C. A custom behavioral indicator of compromise (BIOC) added to a Restriction profile

- D. A correlation rule added to an Agent Blocking profile

正解：C

解説：
In Cortex XDR,custom prevention rulesare used to block specific behaviors or activities on endpoints by leveragingBehavioral Indicators of Compromise (BIOCs). BIOCs define patterns of behavior (e.g., specific process executions, file modifications, or network activities) that, when detected, can trigger preventive actions, such as blocking a process or isolating an endpoint. These BIOCs are typically associated with a Restriction profile, which enforces blocking actions for matched behaviors.
* Correct Answer Analysis (C):Acustom behavioral indicator of compromise (BIOC)added to a Restriction profileenables a custom prevention rule to block specific behavior. The BIOC defines the behavior to detect (e.g., a process accessing a sensitive file), and the Restriction profile specifies the preventive action (e.g., block the process). This configuration ensures that the identified behavior is blocked on endpoints where the profile is applied.
* Why not the other options?
* A. A correlation rule added to an Agent Blocking profile: Correlation rules are used to generate alerts by correlating events across datasets, not to block behaviors directly. There is no
"Agent Blocking profile" in Cortex XDR; this is a misnomer.
* B. A custom behavioral indicator of compromise (BIOC) added to an Exploit profile:
Exploit profiles are used to detect and prevent exploit-based attacks (e.g., memory corruption), not general behavioral patterns defined by BIOCs. BIOCs are associated with Restriction profiles for blocking behaviors.
* D. A correlation rule added to a Malware profile: Correlation rules do not directly block behaviors; they generate alerts. Malware profiles focus on file-based threats (e.g., executables analyzed by WildFire), not behavioral blocking via BIOCs.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains BIOC and Restriction profiles: "Custom BIOCs can be added to Restriction profiles to block specific behaviors on endpoints, enabling tailored prevention rules" (paraphrased from the BIOC and Restriction Profile sections). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers prevention rules, stating that "BIOCs in Restriction profiles enable blocking of specific endpoint behaviors" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing BIOC and prevention rule configuration.
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

質問 # 47
Based on the SBAC scenario image below, when the tenant is switched to permissive mode, which endpoint (s) data will be accessible?



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

正解：A

解説：
In Cortex XDR,Scope-Based Access Control (SBAC)restricts user access to data based on predefined scopes, which can be assigned to endpoints, users, or other resources. Inpermissive mode, SBAC allows users to access data within their assigned scopes but may restrict access to data outside those scopes. The question assumes an SBAC scenario with four endpoints (E1, E2, E3, E4), where the user likely has access to a specific scope (e.g., Scope A) that includes E1, E2, and E3, while E4 is in a different

scope (e.g., Scope B).
* Correct Answer Analysis (C):When the tenant is switched to permissive mode, the user will have access toE1, E2, and E3because these endpoints are within the user's assigned scope (e.g., Scope A).
E4, being in a different scope (e.g., Scope B), will not be accessible unless the user has explicit accessto that scope. Permissive mode enforces scope restrictions, ensuring that only data within the user's scope is visible.
* Why not the other options?
* A. E1 only: This is too restrictive; the user's scope includes E1, E2, and E3, not just E1.
* B. E2 only: Similarly, this is too restrictive; the user's scope includes E1, E2, and E3, not just E2.
* D. E1, E2, E3, and E4: This would only be correct if the user had access to both Scope A and Scope B or if permissive mode ignored scope restrictions entirely, which it does not. Permissive mode still enforces SBAC rules, limiting access to the user's assigned scopes.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains SBAC: "In permissive mode, Scope-Based Access Control restricts user access to endpoints within their assigned scopes, ensuring data visibility aligns with scope permissions" (paraphrased from the Scope-Based Access Control section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers SBAC configuration, stating that "permissive mode allows access to endpoints within a user's scope, such as E1, E2, and E3, while restricting access to endpoints in other scopes" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheet includes "post-deployment management and configuration" as a key exam topic, encompassing SBAC settings.
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

質問 # 48
......

試験を受けることでPalo Alto Networks認定を取得することを期待する人が増えています。ただし、多くの人にとって試験は非常に困難です。特に正しい学習教材を選択せずに適切な方法を見つけた場合、XDR-Engineer試験に合格して関連する認定を取得することはより困難になります。関連する認定を効率的な方法で取得したい場合は、当社のXDR-Engineer学習教材を選択してください。弊社のXDR-Engineer学習教材が試験に合格し、簡単に認定を取得するのに役立ちます。

XDR-Engineer復習テキスト: https://www.jptestking.com/XDR-Engineer-exam.html

- XDR-Engineer復習資料 □ XDR-Engineer試験対応 □ XDR-Engineer試験対応 □ ▹ www.shikenpass.com ◃に移動し、✔ XDR-Engineer □✔□を検索して無料でダウンロードしてくださいXDR-Engineer最新日本語版参考書
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, zbx244.blogspot.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

ちなみに、JPTestKing XDR-Engineerの一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1-1maPyEtXbj2e98577oX_9aigccuMTYK