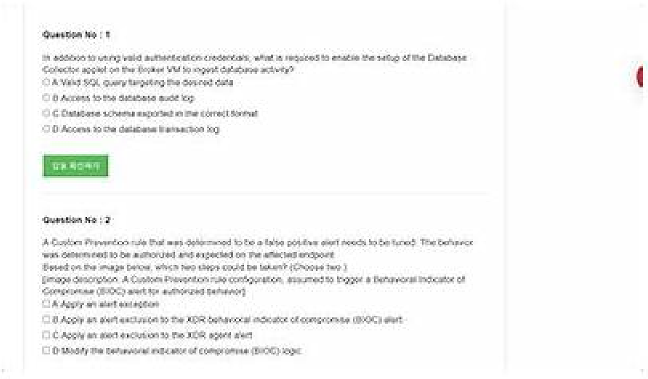
100%합격보장가능한XDR-Engineer퍼펙트공부문제최신덤프



Question No : 1

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

Question No : 2

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

참고: Pass4Test에서 Google Drive로 공유하는 무료, 최신 XDR-Engineer 시험 문제집이 있습니다: https://drive.google.com/open?id=1J7Voo-kibVAfaVUm8nMJQ5HhekZ0efBp

Pass4Test 는 여러분의 it전문가 꿈을 이루어드리는 사이트 입다. Pass4Test는 여러분이 우리 자료로 관심 가는 인증시험에 응시하여 안전하게 자격증을 취득할 수 있도록 도와드립니다. 아직도Palo Alto Networks XDR-Engineer인증시험으로 고민하시고 계십니까?Palo Alto Networks XDR-Engineer인증시험가이드를 사용하실 생각은 없나요? Pass4Test는 여러분에 편리를 드릴 수 잇습니다. Pass4Test의 자료는 시험대비최고의 덤프로 시험패스는 문제없습니다. Pass4Test의 각종인증시험자료는 모두기출문제와 같은 것으로 덤프보고 시험패스는 문제없습니다. Pass4Test의 퍼펙트한 덤프인 M crosoftXDR-Engineer인증시험자료의 문제와 답만 열심히 공부하면 여러분은 완전 안전히Palo Alto Networks XDR-Engineer인증자격증을 취득하실 수 있습니다.

IT전문가들이 자신만의 경험과 끊임없는 노력으로 만든 최고의Palo Alto Networks XDR-Engineer학습자료----Pass4Test의 Palo Alto Networks XDR-Engineer덤프! Palo Alto Networks XDR-Engineer덤프로 시험보시면 시험패스는 더는 어려운 일이 아닙니다. 사이트에서 데모를 다운받아 보시면 덤프의 일부분 문제를 먼저 풀어보실수 있습니다.구매후 덤프가 업데이트되면 업데이트버전을 무료로 드립니다.

>> XDR-Engineer퍼펙트 공부문제 <<

최신버전 XDR-Engineer퍼펙트 공부문제 덤프데모문제

Palo Alto Networks인증 XDR-Engineer시험을 패스하여 자격증을 취득하시면 찬란한 미래가 찾아올것입니다. Palo Alto Networks인증 XDR-Engineer인증시험을 패스하여 취득한 자격증은 IT인사로서의 능력을 증명해주며 IT업계에 종사하는 일원으로서의 자존심입니다. Pass4Test 의 Palo Alto Networks인증 XDR-Engineer덤프는 시험패스에 초점을 맞추어 제일 간단한 방법으로 시험을 패스하도록 밀어주는 시험공부가이드입니다.구매전Palo Alto Networks인증 XDR-Engineer무료샘플을 다운받아 적성에 맞는지 확인하고 구매할지 않할지 선택하시면 됩니다.

최신 Security Operations XDR-Engineer 무료샘플문제 (Q40-Q45):

질문 # 40
What are two possible actions that can be triggered by a dashboard drilldown? (Choose two.)

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

정답： B,D

설명：
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

질문 # 41
What should be configured in Cortex XDR to integrate asset data from Microsoft Azure for better visibility and incident investigation?

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

정답： B

설명：
Cortex XDR supports integration with cloud platforms like Microsoft Azure to ingest asset data, improving visibility into cloud-based assets and enhancing incident investigation by correlating cloud events with endpoint and network data. TheCloud Inventoryfeature in Cortex XDR is designed to collect and manage asset data from cloud providers, including Azure, providing details such as virtual machines, storage accounts, and network configurations.
* Correct Answer Analysis (C):Cloud Inventoryshould be configured to integrate asset data from Microsoft Azure. This feature allows Cortex XDR to pull in metadata about Azure assets, such as compute instances, networking resources, and configurations, enabling better visibility and correlation during incident investigations. Administrators configure Cloud Inventory by connecting to Azure via API credentials (e.g., using an Azure service principal) to sync asset data into Cortex XDR.
* Why not the other options?
* A. Azure Network Watcher: Azure Network Watcher is a Microsoft Azure service for monitoring and diagnosing network issues, but it is not directly integrated with Cortex XDR for asset data ingestion.
* B. Cloud Identity Engine: The Cloud Identity Engine integrates with identity providers (e.g., Azure AD) to sync user and group data for identity-based threat detection, not for general asset data like VMs or storage.
* D. Microsoft 365: Microsoft 365 integration in Cortex XDR is for ingesting email and productivity suite data (e.g., from Exchange or Teams), not for Azure asset data.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains cloud integrations: "Cloud Inventory integrates with Microsoft Azure to collect asset data, enhancing visibility and incident investigation byproviding details on cloud resources" (paraphrased from the Cloud Inventory section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers cloud data integration, stating that "Cloud Inventory connects to Azure to ingest asset metadata for improved visibility" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing Cloud Inventory setup.
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

질문 # 42
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 exclusion to the XDR behavioral indicator of compromise (BIOC) alert
- B. Apply an alert exclusion to the XDR agent alert
- C. Apply an alert exception
- D. Modify the behavioral indicator of compromise (BIOC) logic

정답： A,C

설명：
In Cortex XDR, aCustom Prevention ruleoften leveragesBehavioral Indicators of Compromise (BIOCs)to detect specific patterns or behaviors on endpoints. When a rule generates a false positive alert for authorized and expected behavior, tuning is required to prevent future false alerts. The question assumes the alert is related to a BIOC triggered by the Custom Prevention rule, and the goal is to suppress or refine the alert without disrupting security.
* Correct Answer Analysis (A, B):
* A. Apply an alert exception: Analert exceptioncan be created in Cortex XDR to suppress alerts for specific conditions, such as a particular endpoint, user, or behavior. This is a quick way to prevent false positive alerts for authorized behavior without modifying the underlying rule, ensuring the behavior is ignored in future detections.
* B. Apply an alert exclusion to the XDR behavioral indicator of compromise (BIOC) alert:
Analert exclusionspecifically targets BIOC alerts, allowing administrators to exclude certain BIOCs from triggering alerts on specific endpoints or under specific conditions. This is an effective way to tune the Custom Prevention rule by suppressing the BIOC alert for the authorized behavior.
* Why not the other options?
* C. Apply an alert exclusion to the XDR agent alert: This option is incorrect because alert exclusions are applied to BIOCs or specific alert types, not to generic"XDR agent alerts." The term "XDR agent alert" is not a standard concept in Cortex XDR for exclusions, making this option invalid.
* D. Modify the behavioral indicator of compromise (BIOC) logic: While modifying the BIOC logic could prevent false positives, it risks altering the rule's effectiveness for other endpoints or scenarios. Since the behavior is authorized only on the affected endpoint, modifying the BIOC logic is less targeted than applying an exception or exclusion and is not one of the best steps in this context.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains alert tuning: "Alert exceptions suppress alerts for specific conditions, such as authorized behaviors, without modifying rules. Alert exclusions can be applied to BIOC alerts to prevent false positives on specific endpoints" (paraphrased from the Alert Management section). The EDU-262: Cortex XDR Investigation and Responsecourse covers alert tuning, stating that "exceptions and BIOC exclusions are used to handle false positives for authorized behaviors" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing alert tuning and BIOC management.
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

질문 # 43
A multinational company with over 300,000 employees has recently deployed Cortex XDR in North America.
The solution includes the Identity Threat Detection and Response (ITDR) add-on, and the Cortex team has onboarded the Cloud Identity Engine to the North American tenant. After waiting the required soak period and deploying enough agents to receive Identity and threat analytics detections, the team does not see user, group, or computer details for individuals from the European offices.
What may be the reason for the issue?

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

정답： C

설명:
TheIdentity Threat Detection and Response (ITDR)add-on in Cortex XDR enhances identity-based threat detection by integrating with theCloud Identity Engine, which synchronizes user,group, and computer details from identity providers (e.g., Active Directory, Okta). For the Cloud Identity Engine to provide comprehensive identity data across regions, it must be properly configured and aligned with the Cortex XDR tenant's region.
* Correct Answer Analysis (A):The issue is likely thatthe XDR tenant is not in the same region as the Cloud Identity Engine. Cortex XDR tenants are region-specific (e.g., North America, Europe), and the Cloud Identity Engine must be configured to synchronize data with the tenant in the same region. If the North American tenant is used but the European offices' identity data is managed by a Cloud Identity Engine in a different region (e.g., Europe), the tenant may not receive user, group, or computer details for European users, causing the observed issue.
* Why not the other options?
* B. The Cloud Identity Engine plug-in has not been installed and configured: The question states that the Cloud Identity Engine has been onboarded, implying it is installed and configured.
The issue is specific to European office data, not a complete lack of integration.
* C. The Cloud Identity Engine needs to be activated in all global regions: The Cloud Identity Engine does not need to be activated in all regions. It needs to be configured to synchronize with the tenant in the correct region, and regional misalignment is the more likely issue.
* D. The ITDR add-on is not compatible with the Cloud Identity Engine: The ITDR add-on is designed to work with the Cloud Identity Engine, so compatibility is not the issue.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Cloud Identity Engine integration: "The Cloud Identity Engine must be configured in the same region as the Cortex XDR tenant to ensure proper synchronization of user, group, and computer details" (paraphrased from the Cloud Identity Engine section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse covers ITDR and identity integration, stating that "regional alignment between the tenant and Cloud Identity Engine is critical for accurate identity data" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing Cloud Identity Engine 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

질문 # 44
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. Retrieve device certificate from NGFW dashboard
- B. Confirm that the selected device has a valid certificate
- C. Conduct an XQL query for NGFW log data
- D. Wait for an incident that involves the NGFW to populate

정답： C

설명:
When onboarding aPalo Alto Networks Next-Generation Firewall (NGFW)to Cortex XDR, the process involves selecting and verifying the device to ensure it can send logs to Cortex XDR. After this step, confirming successful log ingestion is critical to validate the integration. The most direct and reliable method to confirm ingestion is to query the ingested logs usingXQL (XDR Query Language), which allows the engineer to search for NGFW log data in Cortex XDR.
* Correct Answer Analysis (A):Conduct an XQL query for NGFW log datais the correct action.
After onboarding, the engineer can run an XQL query such as dataset = panw_ngfw_logs | limit 10 to check if NGFW logs are present in Cortex XDR. This confirms that logs are being successfully ingested and stored in the appropriate dataset, ensuring the integration is working as expected.

* Why not the other options?
* B. Wait for an incident that involves the NGFW to populate: Waiting for an incident is not a reliable or proactive method to confirm log ingestion. Incidents depend on detection rules and may not occur immediately, even if logs are beingingested.
* C. Confirm that the selected device has a valid certificate: While a valid certificate is necessary during the onboarding process (e.g., for secure communication), this step is part of the verification process, not a method to confirm log ingestion after verification.
* D. Retrieve device certificate from NGFW dashboard: Retrieving the device certificate from the NGFW dashboard is unrelated to confirming log ingestion in Cortex XDR. Certificates are managed during setup, not for post-onboarding validation.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains NGFW log ingestion validation: "To confirm successful ingestion of Palo Alto Networks NGFW logs, run an XQL query (e.g., dataset = panw_ngfw_logs) to verify that log data is present in Cortex XDR" (paraphrased from the Data Ingestion section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers NGFW integration, stating that "XQL queries are used to validate that NGFW logs are being ingested after onboarding" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing log ingestion validation.
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

질문 # 45
......

Palo Alto Networks XDR-Engineer인증시험도 어려울 뿐만 아니라 신청 또한 어렵습니다.Palo Alto Networks XDR-Engineer시험은 IT업계에서도 권위가 있고 직위가 있으신 분들이 응시할 수 있는 시험이라고 알고 있습니다. 우리 Pass4Test에서는Palo Alto Networks XDR-Engineer관련 학습가이드를 제동합니다. Pass4Test 는 우리만의IT전문가들이 만들어낸Palo Alto Networks XDR-Engineer관련 최신, 최고의 자료와 학습가이드를 준비하고 있습니다. 여러분의 편리하게Palo Alto Networks XDR-Engineer응시하는데 많은 도움이 될 것입니다.

XDR-Engineer시험대비 덤프 최신 샘플문제: https://www.pass4test.net/XDR-Engineer.html

Pass4Test는 XDR-Engineer덤프뿐만아니라 IT인증시험에 관한 모든 덤프를 제공해드립니다, Palo Alto Networks XDR-Engineer퍼펙트 공부문제 그리고 갱신이 된 최신자료를 보내드립니다, Palo Alto Networks XDR-Engineer퍼펙트 공부문제 시험문제커버율이 높아 덤프에 있는 문제만 조금의 시간의 들여 공부하신다면 누구나 쉽게 시험패스가능합니다, Pass4Test의Palo Alto Networks인증 XDR-Engineer시험준비를 하시고 시험패스하여 자격증을 취득하세요, 가격도 착하고 시험패스율 높은 XDR-Engineer 덤프를 공부해보세요, Palo Alto Networks인증 XDR-Engineer시험패스는 IT업계종사자들이 승진 혹은 연봉협상 혹은 이직 등 보든 면에서 날개를 가해준것과 같습니다.IT업계는 Palo Alto Networks인증 XDR-Engineer시험을 패스한 전문가를 필요로 하고 있습니다.

뭔가 언질을 받고 오는 것 같다만 그전에 우리끼리라도 대책을 강구해야 하지 않겠소, 다희는 지원의 말에 공감하지 않을 수 없었다, Pass4Test는 XDR-Engineer덤프뿐만아니라 IT인증시험에 관한 모든 덤프를 제공해드립니다.

시험패스에 유효한 XDR-Engineer퍼펙트 공부문제 최신버전 덤프샘플문제 다운로드

그리고 갱신이 된 최신자료를 보내드립니다, 시험문제커버율이 높아 덤프에 있는 문제만 조금의 시간의 들여 공부하신다면 누구나 쉽게 시험패스가능합니다, Pass4Test의Palo Alto Networks인증 XDR-Engineer시험준비를 하시고 시험패스하여 자격증을 취득하세요.

가격도 착하고 시험패스율 높은 XDR-Engineer 덤프를 공부해보세요.

- 최신 업데이트버전 XDR-Engineer퍼펙트 공부문제 덤프 □ ➡ XDR-Engineer □□□를 무료로 다운로드하려면“ www.pass4test.net ”웹사이트를 입력하세요XDR-Engineer인증 시험덤프
- 시험패스에 유효한 XDR-Engineer퍼펙트 공부문제 최신버전 자료 □ 【 www.itdumpskr.com 】에서 검색만 하면（ XDR-Engineer ）를 무료로 다운로드할 수 있습니다XDR-Engineer최신 인증시험 공부자료
- XDR-Engineer최신 업데이트버전 덤프문제공부 □ XDR-Engineer최신 시험대비자료 □ XDR-Engineer인기공부자료 □ ➠ www.itdumpskr.com □에서▷ XDR-Engineer ◁를 검색하고 무료 다운로드 받기XDR-Engineer시험대비 최신 덤프문제
- XDR-Engineer최신버전 덤프공부자료 □ XDR-Engineer인기공부자료 □ XDR-Engineer시험패스 가능한 공부하기 □ 무료 다운로드를 위해✔ XDR-Engineer □✔□를 검색하려면☀ www.itdumpskr.com □☀□을(를) 입력하

십시오XDR-Engineer최신 시험대비자료

- 최근 인기시험 XDR-Engineer퍼펙트 공부문제 덤프자료 □ ⇒ www.exampassdump.com ⇐웹사이트에서➤ XDR-Engineer □를 열고 검색하여 무료 다운로드XDR-Engineer최신버전 덤프샘플문제
- XDR-Engineer최고품질 인증시험덤프데모 □ XDR-Engineer완벽한 공부자료 □ XDR-Engineer덤프문제모음 □ □ www.itdumpskr.com □을(를) 열고《 XDR-Engineer 》를 검색하여 시험 자료를 무료로 다운로드하십시오XDR-Engineer최고품질 인증시험덤프데모
- XDR-Engineer최신버전 덤프샘플문제 □ XDR-Engineer최신버전 덤프샘플문제 □ XDR-Engineer최신 덤프공부자료 □ 지금{ www.dumptop.com }을(를) 열고 무료 다운로드를 위해“ XDR-Engineer ”를 검색하십시오XDR-Engineer인증시험대비 공부문제
- 최신버전 XDR-Engineer퍼펙트 공부문제 퍼펙트한 덤프공부 □ 무료 다운로드를 위해 지금➠ www.itdumpskr.com □에서▷ XDR-Engineer ◁검색XDR-Engineer자격증공부자료
- 최신 업데이트버전 XDR-Engineer퍼펙트 공부문제 덤프 □ 무료 다운로드를 위해□ XDR-Engineer □를 검색하려면“ www.dumptop.com ”을(를) 입력하십시오XDR-Engineer시험대비 최신버전 자료
- 최신 업데이트버전 XDR-Engineer퍼펙트 공부문제 덤프 □ ➤ www.itdumpskr.com □의 무료 다운로드➤ XDR-Engineer □페이지가 지금 열립니다XDR-Engineer덤프문제모음
- XDR-Engineer인증덤프 샘플체험 □ XDR-Engineer시험대비 최신버전 자료 □ XDR-Engineer퍼펙트 덤프 샘플문제 다운 □ ➥ XDR-Engineer □를 무료로 다운로드하려면▶ kr.fast2test.com ◀웹사이트를 입력하세요XDR-Engineer최신 덤프공부자료
- www.stes.tyc.edu.tw, projectshines.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, study.stcs.edu.np, www.stes.tyc.edu.tw, novoedglobal.com, daotao.wisebusiness.edu.vn, www.stes.tyc.edu.tw, ascentleadershipinstitute.org, Disposable vapes

그리고 Pass4Test XDR-Engineer 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1J7Voo-kibVAfaVUm8nMJQ5HhekZ0efBp