XDR-Analyst Exam Dumps Collection | Reliable XDR-Analyst Test Simulator

BTW, DOWNLOAD part of ActualVCE XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1PxoVLLY6Rg2-0n_6UcMuJK63xysyt736

Some other top features of ActualVCE XDR-Analyst exam questions are real, valid, and updated Palo Alto Networks XDR Analyst (XDR-Analyst) exam questions, subject matter experts verified Palo Alto Networks XDR Analyst (XDR-Analyst) exam questions, free ActualVCE XDR-Analyst Exam Questions demo download facility, three months updated ActualVCE XDR-Analyst exam questions download facility, affordable price and 100 percent Palo Alto Networks XDR-Analyst exam passing money back guarantee.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
Topic 2	• Endpoint Security Management:
Topic 3	• Data Analysis: This domain encompasses querying data with XQL language, utilizing query templates and libraries, working with lookup tables, hunting for IOCs, using Cortex XDR dashboards, and understanding data retention and Host Insights.
Topic 4	• Incident Handling and Response: This domain focuses on investigating alerts using forensics, causality chains and timelines, analyzing security incidents, executing response actions including automated remediation, and managing exclusions.
Topic 5	• Alerting and Detection Processes: This domain covers identifying alert types and sources, prioritizing alerts through scoring and custom configurations, creating incidents, and grouping alerts with data stitching techniques.

>> XDR-Analyst Exam Dumps Collection <<

Reliable Palo Alto Networks XDR-Analyst Test Simulator & XDR-Analyst Online Test

Obtaining an IT certification shows you are an ambitious individual who is always looking to improve your skill set. Most companies think highly of this character. Our XDR-Analyst exam original questions will help you clear exam certainly in a short time. You don't need to worry about how difficulty the exams are. ActualVCE release the best high-quality XDR-Analyst Exam original questions to help you most candidates pass exams and achieve their goal surely.

Palo Alto Networks XDR Analyst Sample Questions (Q54-Q59):

NEW QUESTION # 54
What contains a logical schema in an XQL query?

- A. Array expand
- B. Field
- C. Dataset
- D. Bin

Answer: B

Explanation:
A logical schema in an XQL query is a field, which is a named attribute of a dataset. A field can have a data type, such as string, integer, boolean, or array. A field can also have a modifier, such as bin or expand, that transforms the field value in the query output. A field can be used in the select, where, group by, order by, or having clauses of an XQL query. Reference:
XQL Syntax
XQL Data Types
XQL Field Modifiers

NEW QUESTION # 55
When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

- A. New
- B. It is blank
- C. Pending
- D. Unassigned

Answer: D

Explanation:
The "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This means that the incident has not been assigned to any analyst or group yet, and it is waiting for someone to take ownership of it. The "assigned to" field is one of the default fields that are displayed in the incident layout, and it can be used to filter and sort incidents in the incident list. The "assigned to" field can be changed manually by an analyst, or automatically by a playbook or a rule12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Pending: This is not the correct answer. Pending is not a valid value for the "assigned to" field. Pending is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
B . It is blank: This is not the correct answer. The "assigned to" field is never blank for any incident. It always has a default value of "Unassigned" for new incidents, unless a playbook or a rule assigns it to a specific analyst or group12.
D . New: This is not the correct answer. New is not a valid value for the "assigned to" field. New is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
In conclusion, the "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This field can be used to manage the ownership and responsibility of incidents, and it can be changed manually or automatically.

Reference:
Cortex XDR Pro Admin Guide: Manage Incidents
Cortex XDR Pro Admin Guide: Assign Incidents
Cortex XDR Pro Admin Guide: Update Incident Status

NEW QUESTION # 56
While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

- A. create a BIOC rule excluding this behavior
- B. mark the incident as Unresolved
- C. create an exception to prevent future false positives
- D. mark the incident as Resolved - False Positive

Answer: D

Explanation:
If all alerts contained in a Cortex XDR incident have exclusions, the Cortex XDR console will automatically mark the incident as Resolved - False Positive. This means that the incident was not a real threat, but a benign or legitimate activity that triggered an alert. By marking the incident as Resolved - False Positive, the Cortex XDR console removes the incident from the list of unresolved incidents and does not count it towards the incident statistics. This helps the analyst to focus on the true positive incidents that require further investigation and response1.
An exclusion is a rule that hides an alert from the Cortex XDR console, based on certain criteria, such as the alert source, type, severity, or description. An exclusion does not change the security policy or prevent the alert from firing, it only suppresses the alert from the console. An exclusion is useful when the analyst wants to reduce the noise of false positive alerts that are not relevant or important2.
An exception, on the other hand, is a rule that overrides the security policy and allows or blocks a process or file from running on an endpoint, based on certain attributes, such as the file hash, path, name, or signer. An exception is useful when the analyst wants to prevent false negative alerts that are caused by malicious or unwanted files or processes that are not detected by the security policy3.
A BIOC rule is a rule that creates an alert based on a custom XQL query that defines a specific behavior of interest or concern. A BIOC rule is useful when the analyst wants to detect and alert on anomalous or suspicious activities that are not covered by the default Cortex XDR rules4.
Reference:
Palo Alto Networks Cortex XDR Documentation, Resolve an Incident1
Palo Alto Networks Cortex XDR Documentation, Alert Exclusions2
Palo Alto Networks Cortex XDR Documentation, Exceptions3
Palo Alto Networks Cortex XDR Documentation, BIOC Rules4

NEW QUESTION # 57
Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

- A. Causality Chain Engine
- B. Causality Analysis Engine
- C. Sensor Engine
- D. Log Stitching Engine

Answer: B

Explanation:
The engine that determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident is the Causality Analysis Engine. The Causality Analysis Engine is one of the core components of Cortex XDR that performs advanced analytics on the data collected from various sources, such as endpoints, networks, and clouds. The Causality Analysis Engine uses machine learning and behavioral analysis to identify the root cause, the attack chain, and the impact of each alert. It also groups related alerts into incidents based on the temporal and logical relationships among the alerts. The Causality Analysis Engine helps to reduce the noise and complexity of alerts and incidents, and provides a clear and concise view of the attack story12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Sensor Engine: This is not the correct answer. The Sensor Engine is not responsible for determining the most relevant artifacts in

each alert and aggregating all alerts related to an event into an incident. The Sensor Engine is the component that runs on the Cortex XDR agents installed on the endpoints. The Sensor Engine collects and analyzes endpoint data, such as processes, files, registry keys, network connections, and user activities. The Sensor Engine also enforces the endpoint security policies and performs prevention and response actions3.
C . Log Stitching Engine: This is not the correct answer. The Log Stitching Engine is not responsible for determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident. The Log Stitching Engine is the component that runs on the Cortex Data Lake, which is the cloud-based data storage and processing platform for Cortex XDR. The Log Stitching Engine normalizes and stitches together the data from different sources, such as firewalls, proxies, endpoints, and clouds. The Log Stitching Engine enables Cortex XDR to correlate and analyze data from multiple sources and provide a unified view of the network activity and threat landscape4.
D . Causality Chain Engine: This is not the correct answer. Causality Chain Engine is not a valid name for any of the Cortex XDR engines. There is no such engine in Cortex XDR that performs the function of determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident.
In conclusion, the Causality Analysis Engine is the engine that determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident. By using the Causality Analysis Engine, Cortex XDR can provide a comprehensive and accurate detection and response capability for security analysts.
Reference:
Cortex XDR Pro Admin Guide: Causality Analysis Engine
Cortex XDR Pro Admin Guide: View Incident Details
Cortex XDR Pro Admin Guide: Sensor Engine
Cortex XDR Pro Admin Guide: Log Stitching Engine

NEW QUESTION # 58
Which statement is correct based on the report output below?

- A. 3,297 total incidents have been detected.
- B. Forensic inventory data collection is enabled.
- C. Host Inventory Data Collection is enabled.
- D. 133 agents have full disk encryption.

Answer: B

Explanation:
The report output shows the number of endpoints that have forensic inventory data collection enabled, which is a feature of Cortex XDR that allows the collection of detailed information about the endpoint's hardware, software, and network configuration. This feature helps analysts to investigate and respond to incidents more effectively by providing a comprehensive view of the endpoint's state and activity. Forensic inventory data collection can be enabled or disabled per policy in Cortex XDR. Reference:
Forensic Inventory Data Collection
Cortex XDR 3: Getting Started with Endpoint Protection

NEW QUESTION # 59
.....

Assist you Clear Exam □ Open website ✔ www.dumpsmaterials.com □✔□ and search for ✔ XDR-Analyst □✔□ for free download □Accurate XDR-Analyst Study Material

- XDR-Analyst Exam Dumps Provider □ New XDR-Analyst Test Guide □ Dumps XDR-Analyst Torrent □ Copy URL ➽ www.pdfvce.com □ open and search for ⇛ XDR-Analyst ⇚ to download for free □Reliable XDR-Analyst Test Vce
- Reliable XDR-Analyst Test Vce □ Accurate XDR-Analyst Study Material □ Dumps XDR-Analyst Torrent □ Copy URL 【 www.prepawaypdf.com 】 open and search for ▹ XDR-Analyst ◃ to download for free □Reliable XDR-Analyst Exam Camp
- Palo Alto Networks XDR-Analyst Exam Dumps Collection: Palo Alto Networks XDR Analyst - Pdfvce Assist you Clear Exam □ Simply search for 【 XDR-Analyst 】 for free download on □ www.pdfvce.com □ □XDR-Analyst Study Guide
- Valid Exam XDR-Analyst Preparation □ XDR-Analyst Preparation □ XDR-Analyst Printable PDF □ Search on ➡ www.torrentvce.com □□□ for ➤ XDR-Analyst □ to obtain exam materials for free download □Dumps XDR-Analyst Torrent
- XDR-Analyst Exam Introduction □ Dumps XDR-Analyst Torrent □ XDR-Analyst Valid Exam Guide □ Go to website ➥ www.pdfvce.com □ open and search for ➤ XDR-Analyst □ to download for free □Test XDR-Analyst Cram Pdf
- The best Palo Alto Networks certification XDR-Analyst exam training mode released □ The page for free download of ➥ XDR-Analyst □ on □ www.pass4test.com □ will open immediately □XDR-Analyst New Braindumps Pdf
- Pass Guaranteed 2026 Palo Alto Networks XDR-Analyst: Marvelous Palo Alto Networks XDR Analyst Exam Dumps Collection □ Search on ▹ www.pdfvce.com ◃ for 「 XDR-Analyst 」 to obtain exam materials for free download □XDR-Analyst New Braindumps Pdf
- Marvelous XDR-Analyst Exam Dumps Collection Help You to Get Acquainted with Real XDR-Analyst Exam Simulation □ □ Simply search for ➤ XDR-Analyst □ for free download on { www.prep4sures.top } □Valid Exam XDR-Analyst Preparation
- 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, app.gxbs.net, teachsmart.asia, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, dahann.com.tw, Disposable vapes

What's more, part of that ActualVCE XDR-Analyst dumps now are free: https://drive.google.com/open?id=1PxoVLLY6Rg2-0n_6UcMuJK63xysyt736