Pass Guaranteed Quiz 2026 XDR-Analyst: Palo Alto Networks XDR Analyst–Professional Dumps Download

BTW, DOWNLOAD part of PDF4Test XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1Y3mja-ubKABgaKp7ZMaYBj39OFSop5GR

With the help of our XDR-Analyst test material, users will learn the knowledge necessary to obtain the Palo Alto Networks certificate and be competitive in the job market and gain a firm foothold in the workplace. Our XDR-Analyst quiz guide' reputation for compiling has created a sound base for our beautiful future business. We are clearly concentrated on the international high-end market, thereby committing our resources to the specific product requirements of this key market sector, as long as cater to all the users who wants to get the test Palo Alto Networks certification.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• Endpoint Security Management: This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
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.

Reliable XDR-Analyst Exam Registration, XDR-Analyst Test Quiz

Our product boosts many merits and high passing rate. Our products have 3 versions and we provide free update of the Palo Alto Networks exam torrent to you. If you are the old client you can enjoy the discounts. Most important of all, as long as we have compiled a new version of the XDR-Analyst Exam Questions, we will send the latest version of our Palo Alto Networks exam questions to our customers for free during the whole year after purchasing. Our product can improve your stocks of knowledge and your abilities in some area and help you gain the success in your career.

Palo Alto Networks XDR Analyst Sample Questions (Q66-Q71):

NEW QUESTION # 66
What is the action taken out by Managed Threat Hunting team for Zero Day Exploits?

- A. MTH researches for threats in the logs and reports to engineering.
- B. MTH researches for threats in the tenant and generates a report with the findings.
- C. MTH pushes content updates to prevent against the zero-day exploits.
- D. MTH runs queries and investigative actions and no further action is taken.

Answer: B

Explanation:
The Managed Threat Hunting (MTH) team is a group of security experts who proactively hunt for threats in the Cortex XDR tenant and generate a report with the findings. The MTH team uses advanced queries and investigative actions to identify and analyze potential threats, such as zero-day exploits, that may have bypassed the prevention and detection capabilities of Cortex XDR. The MTH team also provides recommendations and best practices to help customers remediate the threats and improve their security posture. Reference:
Managed Threat Hunting Service
Managed Threat Hunting Report

NEW QUESTION # 67
Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

- A. a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"
- B. a central system, available via the internet, for registering officially licensed versions of software to prove ownership
- C. a hierarchical database that stores settings for the operating system and for applications
- D. a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Answer: C

Explanation:
The Windows Registry is a hierarchical database that stores settings for the operating system and for applications that run on Windows. The registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. The registry is organized into five main sections, called hives, each of which contains keys, subkeys, and values. The Cortex XDR agent uses the registry to store its configuration, status, and logs, as well as to monitor and control the endpoint's security features. The Cortex XDR agent also allows you to run scripts that can read, write, or delete registry keys and values on the endpoint. Reference:
Windows Registry - Wikipedia
Registry Operations

NEW QUESTION # 68
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. mark the incident as Unresolved
- B. create a BIOC rule excluding this behavior
- 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 # 69
In the Cortex XDR console, from which two pages are you able to manually perform the agent upgrade action? (Choose two.)

- A. Endpoint Administration
- B. Action Center
- C. Asset Management
- D. Agent Installations

Answer: A,C

Explanation:
To manually upgrade the Cortex XDR agents, you can use the Asset Management page or the Endpoint Administration page in the Cortex XDR console. On the Asset Management page, you can select one or more endpoints and click Actions > Upgrade Agent. On the Endpoint Administration page, you can select one or more agent versions and click Upgrade. You can also schedule automatic agent upgrades using the Agent Installations page. Reference:
Asset Management
Endpoint Administration
Agent Installations

NEW QUESTION # 70
A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

- A. It is a false negative.
- B. It is false positive.
- C. It is true negative.
- D. It is true positive.

Answer: B

Explanation:
A false positive is a situation where a file or activity is incorrectly identified as malicious by a security tool, when in fact it is benign or harmless. A false positive can cause unnecessary alerts, disruptions, or remediation actions, and reduce the confidence and efficiency of the security system. In this question, a file is identified as malware by the Local Analysis module, whereas WildFire verdict is Benign, assuming WildFire is accurate. This means that the Local Analysis module has made a mistake and flagged a legitimate file as malicious, while WildFire has correctly determined that the file is safe. Therefore, this is an example of a false positive. The Local Analysis module is a feature of the Cortex XDR agent that uses a static set of pattern-matching rules and a statistical model to determine if an unknown file is likely to be malware. The Local Analysis module can provide a fast and offline verdict for files that are not yet analyzed by WildFire, but it is not as accurate or comprehensive as WildFire, which uses dynamic analysis and machine learning to examine the behavior and characteristics of files in a sandbox environment. WildFire verdicts are considered more reliable and authoritative than Local Analysis verdicts, and can override them in case of a discrepancy. Therefore, if a file is identified as malware by the Local Analysis module, but as Benign by WildFire, the WildFire verdict should be trusted and the Local Analysis verdict should be disregarded123 Reference:
False positive (security) - Wikipedia
Local Analysis
WildFire Overview

NEW QUESTION # 71
.....

If you can own the certification means that you can do the job well in the area so you can get easy and quick promotion. The latest XDR-Analyst quiz torrent can directly lead you to the success of your career. Our materials can simulate real operation exam atmosphere and simulate exams. The download and install set no limits for the amount of the computers and the persons who use XDR-Analyst Test Prep. The XDR-Analyst test prep mainly help our clients pass the XDR-Analyst exam and gain the certification. The certification can bring great benefits to the clients. The clients can enter in the big companies and earn the high salary. You may double the salary after you pass the XDR-Analyst exam.