Free PDF 2026 High-quality Palo Alto Networks Valid XDR-Analyst Dumps

In order to pass Palo Alto Networks Certification XDR-Analyst Exam disposably, you must have a good preparation and a complete knowledge structure. TestPassed can provide you the resources to meet your need.

There are different ways to achieve the same purpose, and it's determined by what way you choose. A lot of people want to pass Palo Alto Networks certification XDR-Analyst exam to let their job and life improve, but people participated in the Palo Alto Networks Certification XDR-Analyst Exam all knew that Palo Alto Networks certification XDR-Analyst exam is not very simple. In order to pass Palo Alto Networks certification XDR-Analyst exam some people spend a lot of valuable time and effort to prepare, but did not succeed.

>> Valid XDR-Analyst Dumps <<

XDR-Analyst Exam Tests, XDR-Analyst Braindumps, XDR-Analyst Actual Test

TestPassed helps you in doing self-assessment so that you reduce your chances of failure in the examination of Palo Alto Networks XDR Analyst (XDR-Analyst) certification. Similarly, this desktop XDR-Analyst practice exam software of TestPassed is compatible with all Windows-based computers. You need no internet connection for it to function. The Internet is only required at the time of product license validation.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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.

Palo Alto Networks XDR Analyst Sample Questions (Q15-Q20):

NEW QUESTION # 15
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically terminate the threads involved in malicious activity.
- B. Automatically close the connections involved in malicious traffic.
- C. Automatically block the IP addresses involved in malicious traffic.
- D. Automatically kill the processes involved in malicious activity.

Answer: C,D

Explanation:
The "Respond to Malicious Causality Chains" feature in a Cortex XDR Windows Malware profile allows the agent to take automatic actions against network connections and processes that are involved in malicious activity on the endpoint. The feature has two modes: Block IP Address and Kill Process1.
The two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile are:
Automatically kill the processes involved in malicious activity. This can help to stop the malware from spreading or doing any further damage.
Automatically block the IP addresses involved in malicious traffic. This can help to prevent the malware from communicating with its command and control server or other malicious hosts.
The other two options, automatically close the connections involved in malicious traffic and automatically terminate the threads involved in malicious activity, are not specific to "Respond to Malicious Causality Chains". They are general security measures that the agent can perform regardless of the feature.
Reference:
Cortex XDR Agent Security Profiles
Cortex XDR Agent 7.5 Release Notes
PCDRA: What are purposes of "Respond to Malicious Causality Chains" in ...

NEW QUESTION # 16
Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

- A. Hash Verdict Determination
- B. Child Process Protection
- C. Restriction Policy
- D. Behavioral Threat Protection

Answer: A

Explanation:
The first protection module that is checked in the Cortex XDR Windows agent malware protection flow is the Hash Verdict Determination. This module compares the hash of the executable file that is about to run on the endpoint with a list of known malicious hashes stored in the Cortex XDR cloud. If the hash matches a malicious hash, the agent blocks the execution and generates an alert. If the hash does not match a malicious hash, the agent proceeds to the next protection module, which is the Restriction Policy1.
The Hash Verdict Determination module is the first line of defense against malware, as it can quickly and efficiently prevent known threats from running on the endpoint. However, this module cannot protect against unknown or zero-day threats, which have no known hash signature. Therefore, the Cortex XDR agent relies on other protection modules, such as Behavioral Threat Protection, Child Process Protection, and Exploit Protection, to detect and block malicious behaviors and exploits that may occur during the execution of the file1.
Reference:
Palo Alto Networks Cortex XDR Documentation, File Analysis and Protection Flow

NEW QUESTION # 17
The Cortex XDR console has triggered an incident, blocking a vitally important piece of software in your organization that is known to be benign. Which of the following options would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization?

- A. Create an endpoint-specific exception.
- B. Create an individual alert exclusion.
- C. Create a global inclusion.
- D. Create a global exception.

Answer: D

Explanation:
A global exception is a rule that allows you to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR. A global exception applies to all endpoints in your organization that are protected by Cortex XDR. Creating a global exception for a vitally important piece of software that is known to be benign would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization.
To create a global exception, you need to follow these steps:
In the Cortex XDR management console, go to Policy Management > Exceptions and click Add Exception.
Select the Global Exception option and click Next.
Enter a name and description for the exception and click Next.
Select the type of exception you want to create, such as file, process, or behavior, and click Next.
Specify the criteria for the exception, such as file name, hash, path, process name, command line, or behavior name, and click Next.
Review the summary of the exception and click Finish.
Reference:
Create Global Exceptions: This document explains how to create global exceptions to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR.
Exceptions Overview: This document provides an overview of exceptions and how they can be used to fine-tune the Cortex XDR security policy.

NEW QUESTION # 18
Which profiles can the user use to configure malware protection in the Cortex XDR console?

- A. Anti-Malware profile
- B. Malware Detection profile
- C. Malware profile
- D. Malware Protection profile

Answer: D

Explanation:
The user can use the Malware Protection profile to configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints. Reference:
Malware Protection Profile
Endpoint Security Policy

NEW QUESTION # 19
Which statement is true for Application Exploits and Kernel Exploits?

- A. Application exploits leverage kernel vulnerability.
- B. Kernel exploits are easier to prevent then application exploits.
- C. The ultimate goal of any exploit is to reach the application.
- D. The ultimate goal of any exploit is to reach the kernel.

Answer: D

Explanation:
The ultimate goal of any exploit is to reach the kernel, which is the core component of the operating system that has the highest level of privileges and access to the hardware resources. Application exploits are attacks that target vulnerabilities in specific applications, such as web browsers, email clients, or office suites. Kernel exploits are attacks that target vulnerabilities in the kernel itself, such as memory corruption, privilege escalation, or code execution. Kernel exploits are more difficult to prevent and detect than application exploits, because they can bypass security mechanisms and hide their presence from the user and the system. Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8 Palo Alto Networks Cortex XDR Documentation, Exploit Protection Overview

NEW QUESTION # 20
.....