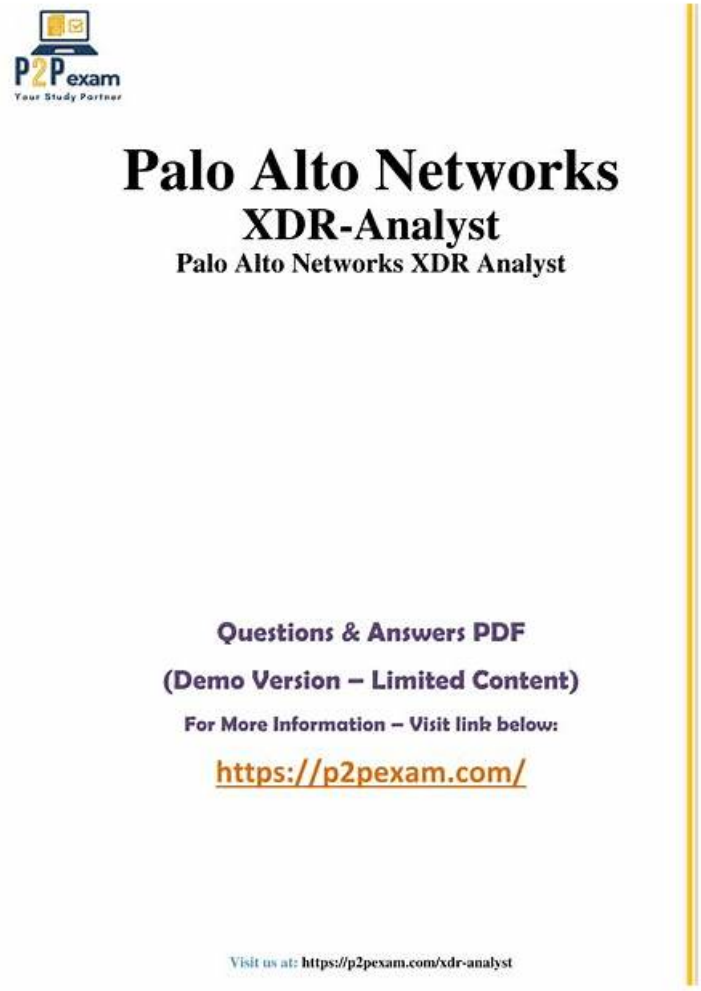
Palo Alto Networks XDR-Analyst Exam | Valid XDR-Analyst Test Cost - Pass Guaranteed for XDR-Analyst: Palo Alto Networks XDR Analyst Exam



There are a lot of advantages if you buy our XDR-Analyst training guide. And one of them is that you can enjoy free updates for one year after purchase. In order to avoid the omission of information, please check your email regularly. The content of XDR-Analyst Exam Materials is very comprehensive, and we are constantly adding new things to it. As long as you purchase XDR-Analyst practice prep, you will not need any other learning products.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 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.

Exam XDR-Analyst Study Guide, Test XDR-Analyst Simulator Free

As the tech industry continues to evolve and adapt to new technologies, professionals who hold the Palo Alto Networks XDR Analyst (XDR-Analyst) certification are better equipped to navigate these changes and stay ahead of the curve, increasing their value to employers and clients. In today's fast-paced and ever-changing Palo Alto Networks sector, having the Palo Alto Networks XDR Analyst (XDR-Analyst) certification has become a necessary requirement for individuals looking to advance their careers and stay competitive in the job market.

Palo Alto Networks XDR Analyst Sample Questions (Q83-Q88):

NEW QUESTION # 83
What is the function of WildFire for Cortex XDR?

- A. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.
- B. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.
- C. WildFire accepts and analyses a sample to provide a verdict.
- D. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.

Answer: C

Explanation:
WildFire is a cloud-based service that accepts and analyses samples from various sources, including Cortex XDR, to provide a verdict of malware, benign, or grayware. WildFire also generates detailed analysis reports that show the behaviour and characteristics of the samples. Cortex XDR uses WildFire verdicts and reports to enhance its detection and prevention capabilities, as well as to provide more visibility and context into the threats. Reference:
WildFire Analysis Concepts
WildFire Overview

NEW QUESTION # 84
When using the "File Search and Destroy" feature, which of the following search hash type is supported?

- A. MD5 hash of the file
- B. AES256 hash of the file
- C. SHA256 hash of the file
- D. SHA1 hash of the file

Answer: C

Explanation:
The File Search and Destroy feature is a capability of Cortex XDR that allows you to search for and delete malicious or unwanted files across your endpoints. You can use this feature to quickly respond to incidents, remediate threats, and enforce compliance policies. To use the File Search and Destroy feature, you need to specify the file name and the file hash of the file you want to search for and delete. The file hash is a unique identifier of the file that is generated by a cryptographic hash function. The file hash ensures that you are targeting the exact file you want, and not a file with a similar name or a different version. The File Search and Destroy feature supports the SHA256 hash type, which is a secure hash algorithm that produces a 256-bit (32-byte) hash value. The SHA256 hash type is widely used for file integrity verification and digital signatures. The File Search and Destroy feature does not support other hash types, such as AES256, MD5, or SHA1, which are either encryption algorithms or less secure hash algorithms. Therefore, the correct answer is A, SHA256 hash of the file1234 Reference:
File Search and Destroy
What is a File Hash?

SHA-2 - Wikipedia
When using the "File Search and Destroy" feature, which of the following search hash type is supported?

NEW QUESTION # 85
Which of the following is an example of a successful exploit?

- A. connecting unknown media to an endpoint that copied malware due to Autorun.
- B. a user executing code which takes advantage of a vulnerability on a local service.
- C. identifying vulnerable services on a server.
- D. executing a process executable for well-known and signed software.

Answer: B

Explanation:
A successful exploit is a piece of software or code that takes advantage of a vulnerability and executes malicious actions on the target system. A vulnerability is a weakness or flaw in a software or hardware component that can be exploited by an attacker. A successful exploit is one that achieves its intended goal, such as gaining unauthorized access, executing arbitrary code, escalating privileges, or compromising data.
In the given options, only B is an example of a successful exploit, because it involves a user executing code that exploits a vulnerability on a local service, such as a web server, a database, or a network protocol. This could allow the attacker to gain control over the service, access sensitive information, or perform other malicious actions.
Option A is not a successful exploit, because it involves connecting unknown media to an endpoint that copied malware due to Autorun. Autorun is a feature that automatically runs a program or script when a removable media, such as a USB drive, is inserted into a computer. This feature can be abused by malware authors to spread their malicious code, but it is not an exploit in itself. The malware still needs to exploit a vulnerability on the endpoint to execute its payload and cause damage.
Option C is not a successful exploit, because it involves identifying vulnerable services on a server. This is a step in the reconnaissance phase of an attack, where the attacker scans the target system for potential vulnerabilities that can be exploited. However, this does not mean that the attacker has successfully exploited any of the vulnerabilities, or that the vulnerabilities are even exploitable.
Option D is not a successful exploit, because it involves executing a process executable for well-known and signed software. This is a legitimate action that does not exploit any vulnerability or cause any harm. Well-known and signed software are programs that are widely used and trusted, and have a digital signature that verifies their authenticity and integrity. Executing such software does not pose a security risk, unless the software itself is malicious or compromised.
Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8 What Is an Exploit? Definition, Types, and Prevention Measures(https://heimdalsecurity.com/blog/what-is-an-exploit/) Exploit Definition & Meaning - Merriam-Webster(https://www.merriam-webster.com/dictionary/exploit)

NEW QUESTION # 86
What is the purpose of the Cortex Data Lake?

- A. a local storage facility where your logs and alert data can be aggregated
- B. the workspace for your Cortex XDR agents to detonate potential malware files
- C. a cloud-based storage facility where your firewall logs are stored
- D. the interface between firewalls and the Cortex XDR agents

Answer: C

Explanation:
The purpose of the Cortex Data Lake is to provide a cloud-based storage facility where your firewall logs are stored. Cortex Data Lake is a service that collects, transforms, and integrates your enterprise's security data to enable Palo Alto Networks solutions. It powers AI and machine learning, detection accuracy, and app and service innovation. Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure, including your next-generation firewalls, Prisma Access, and Cortex XDR. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Cortex Data Lake is available in multiple regions and supports data residency and privacy requirements. Reference:
Cortex Data Lake - Palo Alto Networks
Cortex Data Lake - Palo Alto Networks
Cortex Data Lake, the technology behind Cortex XDR - Palo Alto Networks CORTEX DATA LAKE - Palo Alto Networks
Sizing for Cortex Data Lake Storage - Palo Alto Networks

NEW QUESTION # 87
Which statement is true based on the following Agent Auto Upgrade widget?

- A. Agent Auto Upgrade has not been enabled.
- B. There are more agents in Pending status than In Progress status.
- C. Agent Auto Upgrade was enabled but not on all endpoints.
- D. There are a total of 689 Up To Date agents.

Answer: C

Explanation:
The Agent Auto Upgrade widget shows the status of the agent auto upgrade feature on the endpoints. The widget displays the number of agents that are up to date, in progress, pending, failed, and not configured. In this case, the widget shows that there are 450 agents that are up to date, 78 in progress, 15 pending, 18 failed, and 128 not configured. This means that the agent auto upgrade feature was enabled but not on all endpoints. Reference:
Cortex XDR Agent Auto Upgrade
PCDRA Study Guide

NEW QUESTION # 88
.....

Our XDR-Analyst practice dumps enjoy popularity throughout the world. So with outstanding reputation, many exam candidates have a detailed intervention with our staff before and made a plea for help. We totally understand your mood to achieve success at least the XDR-Analyst Exam Questions right now, so our team makes progress ceaselessly in this area to make better XDR-Analyst study guide for you. We supply both goods which are our XDR-Analyst practice materials as well as high quality services.