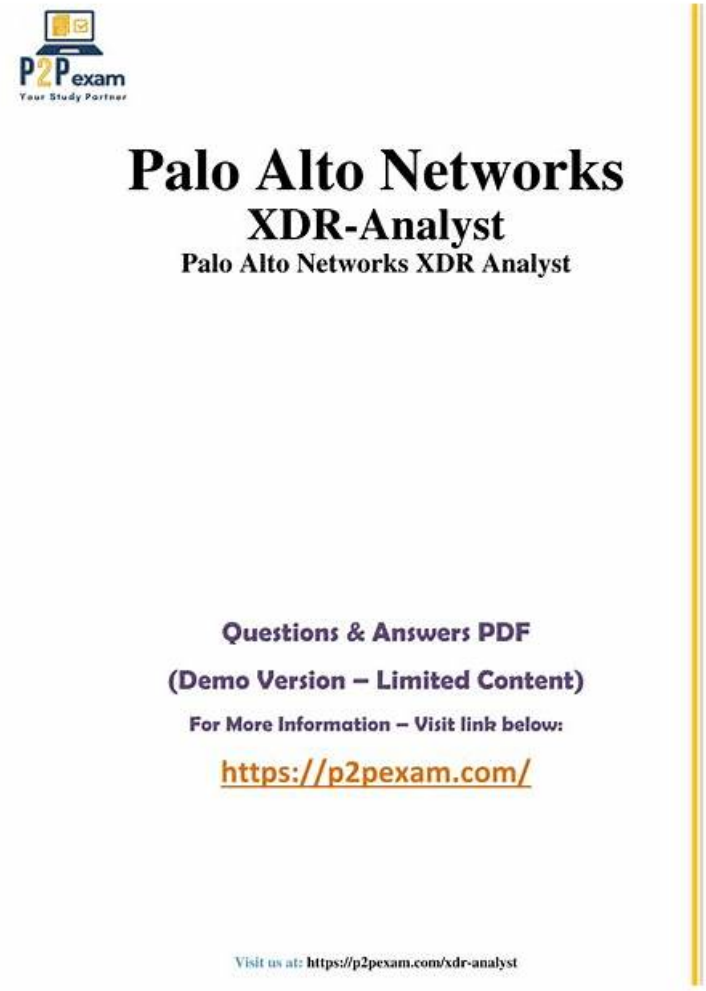
Palo Alto Networks XDR-Analyst Tests & XDR-Analyst Prüfungsmaterialien



Es ist nicht leicht für ITer, die Palo Alto Networks XDR-Analyst IT-Zertifizierungen zu besitzen. Aber Diese Weise ist am besten für sie, ihre Fähigkeit zu entwickeln und ihren Wert zu beweisen. Deshalb müssen viele Leute die Palo Alto Networks XDR-Analyst Prüfungen anmelden. So, gibt es eine einfache Methode, dass sie diese IT-Zertifizierungsprüfungen sehr leicht bestehen. Selbstverständig! Die ZertFragen Dumps ist die beste Wahl. Alle Prüfungsunterlagen sind an ZertFragen vorhanden. Und es kann Ihre Forderungen erfüllen. Sie können sich mehr über die Prüfungsunterlagen an ZertFragen informieren.

Palo Alto Networks XDR-Analyst Prüfungsplan:

Thema	Einzelheiten
Thema 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.
Thema 2	• 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.
Thema 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.

Thema 4	• 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.

>> Palo Alto Networks XDR-Analyst Tests <<

Hohe Qualität von XDR-Analyst Prüfung und Antworten

Mit der Palo Alto Networks XDR-Analyst Zertifizierungsprüfung werden Sie sicher bessere Berufsaussichten haben. Die Palo Alto Networks XDR-Analyst Zertifizierungsprüfung kann nicht nur Ihre Fertigkeiten, sondern auch Ihre Zertifikate und Fachkenntnisse beweisen. Die den Schulungsunterlagen zur Palo Alto Networks XDR-Analyst Zertifizierungsprüfung von ZertFragen sind eine von der Praxis bewährte Software. Mit ihr können Sie eine bessere Theorie bekommen. Vorm Kauf können Sie eine kostenlose Probeversion bekommen. So kennen Sie die Qualität unserer Prüfungsmaterialien. ZertFragen ist Ihnen die beste Wahl.

Palo Alto Networks XDR Analyst XDR-Analyst Prüfungsfragen mit Lösungen (Q49-Q54):

49. Frage
What is the purpose of the Unit 42 team?

- A. Unit 42 is responsible for threat research, malware analysis and threat hunting
- B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server
- C. Unit 42 is responsible for the rapid deployment of Cortex XDR agents
- D. Unit 42 is responsible for automation and orchestration of products

Antwort: A

Begründung:
Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Unit 42 is not responsible for automation and orchestration of products. Automation and orchestration are capabilities that are provided by Palo Alto Networks products such as Cortex XSOAR, which is a security orchestration, automation and response platform that helps security teams automate tasks, coordinate actions and manage incidents3.
B . Unit 42 is not responsible for the configuration optimization of the Cortex XDR server. The Cortex XDR server is the cloud-based platform that provides detection and response capabilities across network, endpoint and cloud data sources. The configuration optimization of the Cortex XDR server is the responsibility of the Cortex XDR administrators, who can use the Cortex XDR app to manage the settings and policies of the Cortex XDR server4.
C . Unit 42 is not responsible for the rapid deployment of Cortex XDR agents. The Cortex XDR agents are the software components that are installed on endpoints to provide protection and visibility. The rapid deployment of Cortex XDR agents is the responsibility of the Cortex XDR administrators, who can use various methods such as group policy objects, scripts, or third-party tools to deploy the Cortex XDR agents to multiple endpoints5.
In conclusion, Unit 42 is the threat intelligence and response team of Palo Alto Networks that is responsible for threat research, malware analysis and threat hunting. By leveraging the expertise and insights of Unit 42, organizations can enhance their security posture and protect against the latest cyberthreats.
Reference:
About Unit 42: Our Mission and Team
Unit 42: Threat Intelligence & Response
Cortex XSOAR
Cortex XDR Pro Admin Guide: Manage Cortex XDR Settings and Policies
Cortex XDR Pro Admin Guide: Deploy Cortex XDR Agents

50. Frage
Which of the following represents the correct relation of alerts to incidents?

- A. Only alerts with the same host are grouped together into one Incident in a given time frame.
- B. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
- C. Every alert creates a new Incident.
- D. Alerts that occur within a three-hour time frame are grouped together into one Incident.

Antwort: B

Begründung:
The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts, such as the alert source, type, and time period, to determine if they belong to the same causality chain. By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details1.
Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack.
Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack.
Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes.
Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, Incident Management Overview2 Cortex XDR: Stop Breaches with AI-Powered Cybersecurity1

51. Frage
Which search methods is supported by File Search and Destroy?

- A. File Search and Destroy
- B. File Seek and Destroy
- C. File Seek and Repair
- D. File Search and Repair

Antwort: A

Begründung:
File Search and Destroy is a feature of Cortex XDR that allows you to search for and remove malicious files from endpoints. You can use this feature to find files by their hash, full path, or partial path using regex parameters. You can then select the files from the search results and destroy them by hash or by path. When you destroy a file by hash, all the file instances on the endpoint are removed. File Search and Destroy is useful for quickly responding to threats and preventing further damage. Reference:
Search and Destroy Malicious Files
Cortex XDR Pro Administrator Guide

52. Frage
Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

- A. in the macOS Malware Protection Profile to indicate allowed signers
- B. in the Windows Malware Protection Profile to indicate allowed executables
- C. SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles
- D. in the Linux Malware Protection Profile to indicate allowed Java libraries

Antwort: B

Begründung:

Cortex XDR Malware Protection Profiles allow you to configure the malware prevention settings for Windows, Linux, and macOS endpoints. You can use SHA256 hash values in the Windows Malware Protection Profile to indicate allowed executables that you want to exclude from malware scanning. This can help you reduce false positives and improve performance by skipping the scanning of known benign files. You can add up to 1000 SHA256 hash values per profile. You cannot use SHA256 hash values in the Linux or macOS Malware Protection Profiles, but you can use other criteria such as file path, file name, or signer to exclude files from scanning. Reference:
Malware Protection Profiles
Configure a Windows Malware Protection Profile
PCDRA Study Guide

53. Frage
Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

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

Antwort: B

Begründung:
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

54. Frage
.....

- XDR-Analyst Übungsmaterialien □ XDR-Analyst PDF Demo □ XDR-Analyst Antworten □ Suchen Sie einfach auf ▸ www.itzert.com ◂ nach kostenloser Download von ☀ XDR-Analyst □☀□ □XDR-Analyst Fragenpool
- Die seit kurzem aktuellsten Palo Alto Networks XDR-Analyst Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der Prüfungen! □ Sie müssen nur zu [www.pass4test.de] gehen um nach kostenloser Download von ✔ XDR-Analyst □✔□ zu suchen □XDR-Analyst Prüfungsfrage
- XDR-Analyst Testing Engine □ XDR-Analyst Lerntipps □ XDR-Analyst Prüfungsmaterialien □ Öffnen Sie die Webseite 《 www.itzert.com 》 und suchen Sie nach kostenloser Download von 「 XDR-Analyst 」 □XDR-Analyst PDF Demo
- Sie können so einfach wie möglich - XDR-Analyst bestehen! □ Suchen Sie auf { www.itzert.com } nach kostenlosem Download von " XDR-Analyst " □XDR-Analyst Übungsmaterialien
- XDR-Analyst Prüfungsmaterialien □ XDR-Analyst Übungsmaterialien □ XDR-Analyst Zertifizierungsprüfung □ Öffnen Sie die Webseite ▸ www.itzert.com ◂ und suchen Sie nach kostenloser Download von ➤ XDR-Analyst □ □XDR-Analyst Testing Engine
- XDR-Analyst Übungsfragen: Palo Alto Networks XDR Analyst - XDR-Analyst Dateien Prüfungsunterlagen □ Geben Sie 【 www.itzert.com 】 ein und suchen Sie nach kostenloser Download von □ XDR-Analyst □ □XDR-Analyst Praxisprüfung
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, free.ulearners.org, 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, Disposable vapes