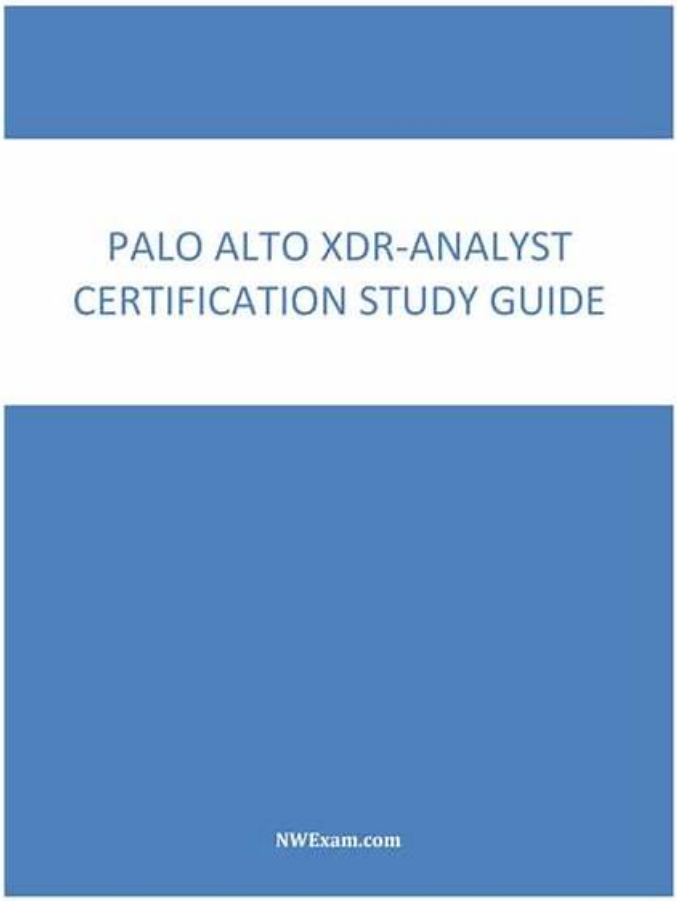
Palo Alto Networks XDR-Analyst Prüfungsunterlagen - XDR-Analyst Schulungsangebot



Warum sind die Fragenkataloge zur Palo Alto Networks XDR-Analyst Zertifizierungsprüfung von ZertSoft beliebter als die anderen? Erstens: Ressonanz. Wir müssen die Bedürfnisse der Kandidaten kennen, und umfassender als andere Websites. Zweitens: Spezialität. Um unsere Angelegenheiten zu erledigen, müssen wir alle unwichtigen Chancen aufgeben. Drittens: Man wird vielleicht eine Sache nach ihrem Aussehen beurteilen. Vielleicht haben wir die besten Produkte von guter Qualität. Aber wenn wir sie in einer kitschig Weise repräsentieren, werden Sie sicher zu den kitschigen Produkten gehören. Hingegen repräsentieren wir sie in einer fachlichen und kreativen Weise werden wir die besten Effekte erzielen. Die Fragenkataloge zur Palo Alto Networks XDR-Analyst Zertifizierungsprüfung von ZertSoft sind solche erfolgreichen Fragenkataloge.

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	• 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.

Thema 3	• 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 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.

>> Palo Alto Networks XDR-Analyst Prüfungsunterlagen <<

XDR-Analyst Schulungsangebot - XDR-Analyst Fragen Und Antworten

Viele Kandidaten wissen einfach nicht, wie sie sich auf die Prüfung vorbereiten können und hilflos sind. Aber mit den Schulungsunterlagen zur Palo Alto Networks XDR-Analyst Zertifizierungsprüfung von ZertSoft ist alles ganz anders geworden. Mit ihr können Sie sich ganz selbstsicher auf Ihre Prüfung vorbereiten. Sie haben kein Risiko, in der Prüfung durchzufallen, mehr zu tragen. Das ist nicht nur seelische Hilfe. Am wichtigsten ist es, dass Sie die Prüfung bestehen und eine glänzende Zukunft haben können.

Palo Alto Networks XDR Analyst XDR-Analyst Prüfungsfragen mit Lösungen (Q79-Q84):

79. Frage
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 true negative.
- C. It is true positive.
- D. It is false positive.

Antwort: D

Begründung:
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

80. Frage
In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

- A. Agent Proxy
- B. Syslog Collector
- C. CSV Collector
- D. Agent Installer and Content Caching

Antwort: D

Begründung:
The Agent Installer and Content Caching applet of the Broker VM is used to download and cache the Cortex XDR agent installation packages and content updates from Palo Alto Networks servers. This applet also acts as a proxy server for the Cortex XDR agents to communicate with the Cortex Data Lake and the Cortex XDR management console. To ensure secure communication between the Broker VM and the Cortex XDR agents, you are required to install a strong cipher SHA256-based SSL certificate on the Broker VM. The SSL certificate must have a common name or subject alternative name that matches the Broker VM FQDN or IP address. The SSL certificate must also be trusted by the Cortex XDR agents, either by using a certificate signed by a public CA or by manually installing the certificate on the endpoints. Reference:
Agent Installer and Content Caching
Install an SSL Certificate on the Broker VM

81. Frage
What should you do to automatically convert leads into alerts after investigating a lead?

- A. Create BIOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.
- B. Build a search query using Query Builder or XQL using a list of IOCs.
- C. Lead threats can't be prevented in the future because they already exist in the environment.
- D. Create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.

Antwort: D

Begründung:
To automatically convert leads into alerts after investigating a lead, you should create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting. IOC rules are used to detect known threats based on indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, etc. By creating IOC rules from the leads, you can prevent future occurrences of the same threats and generate alerts for them. Reference:
PCDRA Study Guide, page 25
Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2
Cortex XDR Documentation, section "Create IOC Rules"

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

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

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

83. Frage
When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information

you need to collect from the Agent? (Choose Two)

- A. The prevention archive from the alert.
- B. The unique agent id.
- C. The distribution id of the agent.
- D. The agent technical support file.
- E. A list of all the current exceptions applied to the agent.

Antwort: A,D

Begründung:
When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:
The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself.
The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself.
The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:
The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.
A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.
The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.
Reference:
Generate and Download the Agent Technical Support File
Generate and Download the Prevention Archive
Cortex XDR Agent Administrator Guide: Agent Distribution ID
Cortex XDR Agent Administrator Guide: Exception Security Profiles
[Cortex XDR Agent Administrator Guide: Unique Agent ID]

84. Frage
.....

Viele IT-Fachleute wollen Palo Alto Networks XDR-Analyst Zertifikate erhalten. Die IT-Zertifikate werden Ihnen helfen, in der IT-Branche befördert zu werden. Das Palo Alto Networks XDR-Analyst Zertifikat ist ein beliebtes unter den vielen Zertifikaten. Obwohl es nicht so leicht ist, die Palo Alto Networks XDR-Analyst Zertifizierungsprüfung zu bestehen, gibt es doch Methoden. Sie können viel Zeit und Energie für die Prüfung benutzen, um Ihr Know-How zu konsolidieren, oder an den effizienten Kursen teilnehmen. Die speziellen Simulationsprüfungen von ZertSoft, die Ihnen viel Zeit und Energie ersparen und Ihr Ziel erreichen können, ist sehr effizient. ZertSoft ist eine gute Wahl für Sie.

www.itzert.com □ nach 【 XDR-Analyst 】 um den kostenlosen Download zu erhalten □XDR-Analyst Deutsch Prüfungsfragen

- XDR-Analyst Examsfragen □ XDR-Analyst Vorbereitungsfragen □ XDR-Analyst Testfagen □ Suchen Sie auf der Webseite { www.zertfragen.com } nach 「 XDR-Analyst 」 und laden Sie es kostenlos herunter □XDR-Analyst Pruefungssimulationen
- XDR-Analyst Ressourcen Prüfung - XDR-Analyst Prüfungsguide - XDR-Analyst Beste Fragen □ ➠ www.itzert.com □ ist die beste Webseite um den kostenlosen Download von ▸ XDR-Analyst ◂ zu erhalten □XDR-Analyst Examengine
- Palo Alto Networks XDR Analyst cexamkiller Praxis Dumps - XDR-Analyst Test Training Überprüfungen □ Suchen Sie auf ➡ www.pruefungfrage.de □□□ nach 「 XDR-Analyst 」 und erhalten Sie den kostenlosen Download mühelos □ □XDR-Analyst Examengine
- XDR-Analyst Exam Fragen □ XDR-Analyst Testfagen □ XDR-Analyst Prüfungsfragen □ Suchen Sie einfach auf ➤ www.itzert.com □ nach kostenloser Download von ➡ XDR-Analyst □□□ □XDR-Analyst Exam Fragen
- XDR-Analyst Testing Engine □ XDR-Analyst Examsfragen □ XDR-Analyst Echte Fragen □ Suchen Sie auf der Webseite ➠ www.itzert.com □ nach ▸ XDR-Analyst ◂ und laden Sie es kostenlos herunter □XDR-Analyst Fragen&Antworten
- XDR-Analyst Exam Fragen □ XDR-Analyst Exam Fragen □ XDR-Analyst Zertifizierung 🗓 Suchen Sie jetzt auf ➡ www.itzert.com □□□ nach ▹ XDR-Analyst ◃ um den kostenlosen Download zu erhalten □XDR-Analyst Prüfungsinformationen
- Hohe Qualität von XDR-Analyst Prüfung und Antworten □ Suchen Sie jetzt auf 《 www.zertsoft.com 》 nach □ XDR-Analyst □ um den kostenlosen Download zu erhalten □XDR-Analyst PDF
- 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, myportal.utt.edu.tt, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes