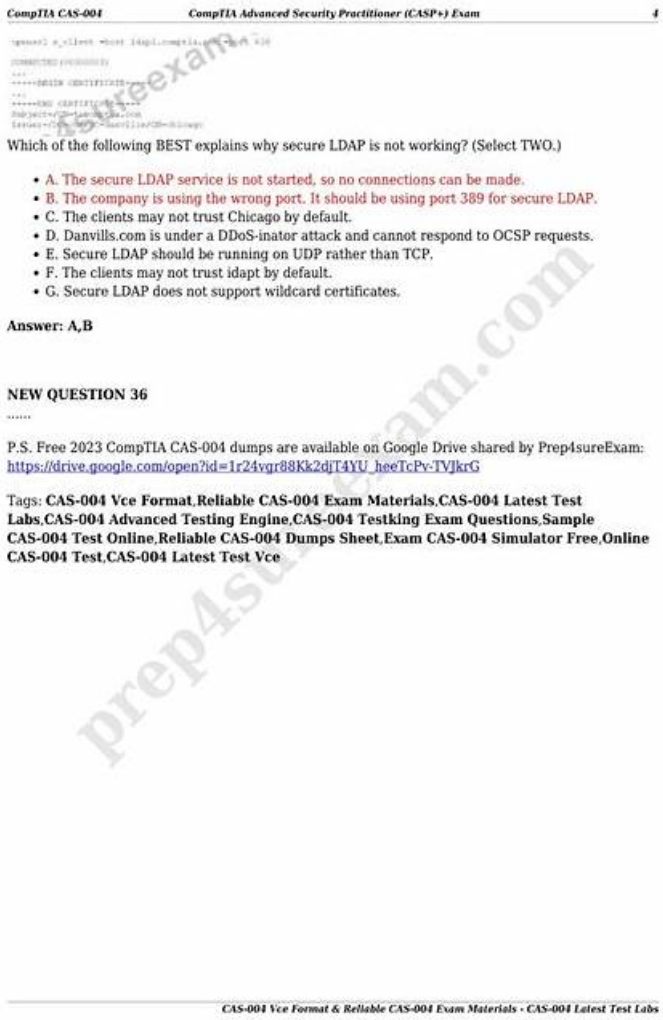
XDR-Analyst Vce Format, Reliable XDR-Analyst Test Dumps



CompTIA CAS-004 CompTIA Advanced Security Practitioner (CASP+) Exam 4

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

- A. The secure LDAP service is not started, so no connections can be made.
- B. The company is using the wrong port. It should be using port 389 for secure LDAP.
- C. The clients may not trust Chicago by default.
- D. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- E. Secure LDAP should be running on UDP rather than TCP.
- F. The clients may not trust idapt by default.
- G. Secure LDAP does not support wildcard certificates.

Answer: A,B

NEW QUESTION 36

.....

P.S. Free 2023 CompTIA CAS-004 dumps are available on Google Drive shared by Prep4sureExam: https://drive.google.com/open?id=1r24vgr88Kk2djT4YU_heeTcPv-TVJkrG

Tags: **CAS-004 Vce Format,Reliable CAS-004 Exam Materials,CAS-004 Latest Test Labs,CAS-004 Advanced Testing Engine,CAS-004 Testking Exam Questions,Sample CAS-004 Test Online,Reliable CAS-004 Dumps Sheet,Exam CAS-004 Simulator Free,Online CAS-004 Test,CAS-004 Latest Test Vce**

CAS-004 Vce Format & Reliable CAS-004 Exam Materials - CAS-004 Latest Test Labs

DOWNLOAD the newest DumpsValid XDR-Analyst PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=10URnaNG6acO47TBcP6kI5Fdhdoqhr6fl

Our Palo Alto Networks XDR-Analyst Exam Dumps effect in helping candidates' certification exam. Original questions are also important. These would provide a forum where certification training can be carried on. Our dumps torrent is perfect and practice test is also the latest. After you purchase our product, we offer free update service for one year.

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	• Endpoint Security Management:
Topic 3	• 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.
Topic 5	• 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 Test Dumps & Latest XDR-Analyst Test Blueprint

You can take the Palo Alto Networks XDR Analyst XDR-Analyst practice exam many times to analyze and overcome your weaknesses before the final Palo Alto Networks XDR Analyst XDR-Analyst exam. You will also improve your time management abilities by learning Palo Alto Networks XDR Analyst in DumpsValid. XDR-Analyst Practice Test software 365 days updated and reliable. You will not face any problems in the final XDR-Analyst exam.

Palo Alto Networks XDR Analyst Sample Questions (Q69-Q74):

NEW QUESTION # 69
In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?

- A. Add the signer to the allow list in the malware profile.
- B. Add the signer to the allow list under the action center page.
- C. Create a new rule exception and use the singer as the characteristic.
- D. In the Restrictions Profile, add the file name and path to the Executable Files allow list.

Answer: A

Explanation:
To prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. A malware profile is a profile that defines the settings and actions for malware prevention and detection on the endpoints. A malware profile allows you to specify a list of files, folders, or signers that you want to exclude from malware scanning and blocking. By adding the signer to the allow list in the malware profile, you can prevent the Cortex XDR Agent from blocking any file that is signed by that signer1.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . In the Restrictions Profile, add the file name and path to the Executable Files allow list: This is not the correct answer. Adding the file name and path to the Executable Files allow list in the Restrictions Profile will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A Restrictions Profile is a profile that defines the settings and actions for restricting the execution of files or processes on the endpoints. A Restrictions Profile allows you to specify a list of executable files that you want to allow or block based on the file name and path. However, this method does not take into account the digital signer of the file, and it may not be effective if the file name or path changes2.
B . Create a new rule exception and use the signer as the characteristic: This is not the correct answer. Creating a new rule exception and using the signer as the characteristic will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A rule exception is an exception that you can create to modify the behavior of a specific prevention rule or BIOC rule. A rule exception allows you to specify the characteristics and the actions that you want to apply to the exception, such as file hash, process name, IP address, or domain name. However, this method does not support using the signer as a characteristic, and it may not be applicable to all prevention rules or BIOC rules3.
D . Add the signer to the allow list under the action center page: This is not the correct answer. Adding the signer to the allow list under the action center page will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. The action center page is a page that allows you to create and manage actions that you can perform on your endpoints, such as isolating, scanning, collecting files, or executing scripts. The action center page does not have an option to add a signer to the allow list, and it is not related to the malware prevention or detection functionality4.
In conclusion, to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. By using this method, you can exclude the files that are signed by the trusted signer from the malware scanning and blocking.
Reference:

Add a New Malware Security Profile
Add a New Restrictions Security Profile
Create a Rule Exception
Action Center

NEW QUESTION # 70
Which Type of IOC can you define in Cortex XDR?

- A. e-mail address
- B. App-ID
- C. destination port
- D. full path

Answer: D

Explanation:
Cortex XDR allows you to define IOCs based on various criteria, such as file hashes, registry keys, IP addresses, domain names, and full paths. A full path IOC is a specific location of a file or folder on an endpoint, such as C:\Windows\System32\calc.exe. You can use full path IOCs to detect and respond to malicious files or folders that are located in known locations on your endpoints12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . destination port: This is not the correct answer. Destination port is not a type of IOC that you can define in Cortex XDR. Destination port is a network attribute that indicates the port number to which a packet is sent. Cortex XDR does not support defining IOCs based on destination ports, but you can use XQL queries to filter network events by destination ports3.
B . e-mail address: This is not the correct answer. E-mail address is not a type of IOC that you can define in Cortex XDR. E-mail address is an identifier that is used to send and receive e-mails. Cortex XDR does not support defining IOCs based on e-mail addresses, but you can use the Cortex XDR - IOC integration with Cortex XSOAR to ingest IOCs from various sources, including e-mail addresses4.
D . App-ID: This is not the correct answer. App-ID is not a type of IOC that you can define in Cortex XDR. App-ID is a feature of Palo Alto Networks firewalls that identifies and controls applications on the network. Cortex XDR does not support defining IOCs based on App-IDs, but you can use the Cortex XDR Analytics app to create custom rules that use App-IDs as part of the rule logic5.
In conclusion, full path is the type of IOC that you can define in Cortex XDR. By using full path IOCs, you can enhance your detection and response capabilities and protect your endpoints from malicious files or folders.
Reference:
Create an IOC Rule
XQL Reference Guide: Network Events Schema
Cortex XDR - IOC
Cortex XDR Analytics App
PCDRA: Which Type of IOC can define in Cortex XDR?

NEW QUESTION # 71
What motivation do ransomware attackers have for returning access to systems once their victims have paid?

- A. Failure to restore access to systems undermines the scheme because others will not believe their valuables would be returned.
- B. The ransomware attackers hope to trace the financial trail back and steal more from traditional banking institutions. -
- C. There is organized crime governance among attackers that requires the return of access to remain in good standing.
- D. Nation-states enforce the return of system access through the use of laws and regulation.

Answer: A

Explanation:
Ransomware attackers have a motivation to return access to systems once their victims have paid because they want to maintain their reputation and credibility. If they fail to restore access to systems, they risk losing the trust of future victims who may not believe that paying the ransom will result in getting their data back. This would reduce the effectiveness and profitability of their scheme. Therefore, ransomware attackers have an incentive to honor their promises and decrypt the data after receiving the ransom.
Reference:
What is the motivation behind ransomware? | Foresite
As Ransomware Attackers' Motives Change, So Should Your Defense - Forbes

NEW QUESTION # 72
What is the outcome of creating and implementing an alert exclusion?

- A. The Cortex XDR agent will not create an alert for this event in the future.
- B. The Cortex XDR console will delete those alerts and block ingestion of them in the future.
- C. The Cortex XDR console will hide those alerts.
- D. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.

Answer: C

Explanation:
The outcome of creating and implementing an alert exclusion is that the Cortex XDR console will hide those alerts that match the exclusion criteria. An alert exclusion is a policy that allows you to filter out alerts that are not relevant, false positives, or low priority, and focus on the alerts that require your attention. When you create an alert exclusion, you can specify the criteria that define which alerts you want to exclude, such as alert name, severity, source, or endpoint. After you create an alert exclusion, Cortex XDR will hide any future alerts that match the criteria, and exclude them from incidents and search query results. However, the alert exclusion does not affect the behavior of the Cortex XDR agent or the security policy on the endpoint. The Cortex XDR agent will still create an alert for the event and apply the appropriate action, such as blocking or quarantining, according to the security policy. The alert exclusion only affects the visibility of the alert on the Cortex XDR console, not the actual protection of the endpoint. Therefore, the correct answer is B, the Cortex XDR console will hide those alerts12 Reference:
Alert Exclusions
Create an Alert Exclusion Policy

NEW QUESTION # 73
Which statement is correct based on the report output below?

- A. Forensic inventory data collection is enabled.
- B. 3,297 total incidents have been detected.
- C. 133 agents have full disk encryption.
- D. Host Inventory Data Collection is enabled.

Answer: A

Explanation:
The report output shows the number of endpoints that have forensic inventory data collection enabled, which is a feature of Cortex XDR that allows the collection of detailed information about the endpoint's hardware, software, and network configuration. This feature helps analysts to investigate and respond to incidents more effectively by providing a comprehensive view of the endpoint's state and activity. Forensic inventory data collection can be enabled or disabled per policy in Cortex XDR. Reference:
Forensic Inventory Data Collection
Cortex XDR 3: Getting Started with Endpoint Protection

NEW QUESTION # 74
.....

- Palo Alto Networks XDR-Analyst Questions: Turn Your Exam Fear into Confidence [2026] □ Search for ☀ XDR-Analyst □☀□ and obtain a free download on ✔ www.pdfdumps.com □✔□ ～XDR-Analyst Lab Questions
- 2026 Palo Alto Networks XDR-Analyst: Latest Palo Alto Networks XDR Analyst Vce Format □ Search for 《 XDR-Analyst 》 and download exam materials for free through " www.pdfvce.com " □XDR-Analyst Certification Torrent
- Don't Fail XDR-Analyst Exam - Verified By www.pdfdumps.com □ Simply search for ▸ XDR-Analyst ◂ for free download on ➥ www.pdfdumps.com □ □Test XDR-Analyst Questions Vce
- XDR-Analyst Latest Test Pdf □ XDR-Analyst Exam Test □ Latest XDR-Analyst Exam Papers □ Enter ➤ www.pdfvce.com □ and search for □ XDR-Analyst □ to download for free □Valid XDR-Analyst Cram Materials
- Pass Guaranteed Updated XDR-Analyst - Palo Alto Networks XDR Analyst Vce Format □ Go to website ▸ www.troytecdumps.com ◂ open and search for ➠ XDR-Analyst □ to download for free □XDR-Analyst Practice Test Fee
- Latest XDR-Analyst Dumps Files □ XDR-Analyst Valid Exam Camp Pdf ☂ XDR-Analyst Valid Exam Camp Pdf □ Search for □ XDR-Analyst □ and easily obtain a free download on □ www.pdfvce.com □ □Test XDR-Analyst Questions Vce
- 100% Pass Quiz 2026 Latest XDR-Analyst: Palo Alto Networks XDR Analyst Vce Format □ Copy URL ✔ www.pass4test.com □✔□ open and search for 「 XDR-Analyst 」 to download for free □XDR-Analyst Certification Torrent
- Pass Guaranteed Updated XDR-Analyst - Palo Alto Networks XDR Analyst Vce Format □ Search for 「 XDR-Analyst 」 and download it for free on ⇛ www.pdfvce.com ⇚ website □Exam XDR-Analyst Answers
- XDR-Analyst Accurate Test □ XDR-Analyst Accurate Test □ Exam XDR-Analyst Answers □ ▸ www.prepawaypdf.com ◂ is best website to obtain 《 XDR-Analyst 》 for free download □Latest XDR-Analyst Dumps Files
- faithlife.com, www.quora.com, freestyler.ws, www.stes.tyc.edu.tw, bbs.chaken.net.cn, issuu.com, www.stes.tyc.edu.tw, justpaste.me, www.huajiaoshu.com, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that DumpsValid XDR-Analyst dumps now are free: https://drive.google.com/open?id=10URnaNG6acO47TBcP6kI5Fdhdoqhr6fl