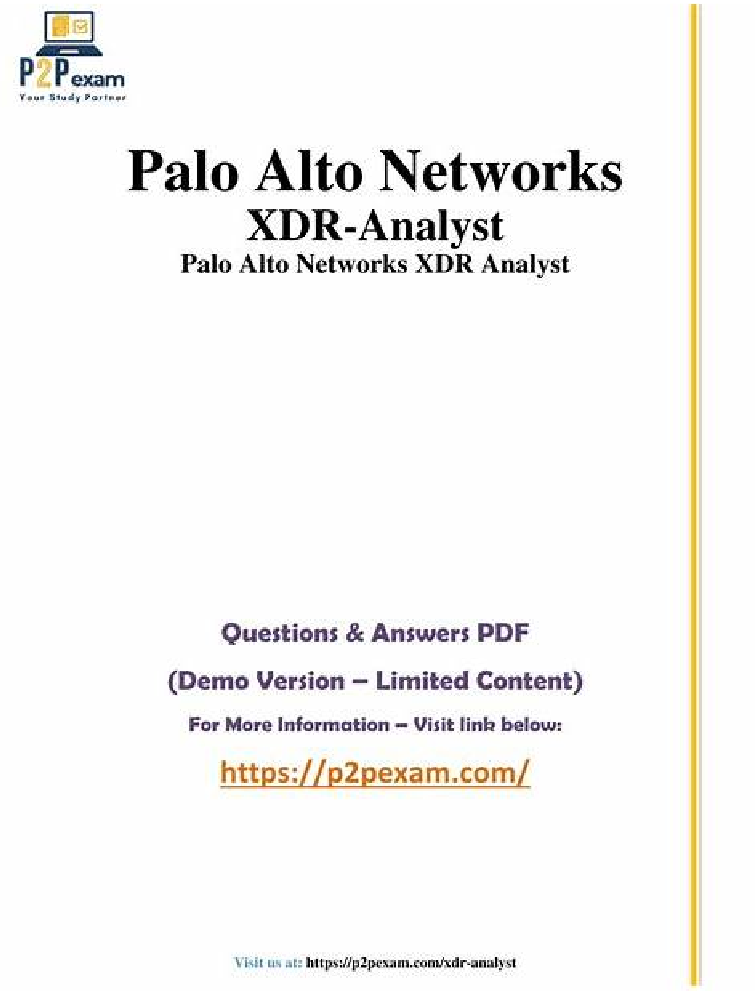
# How Can Palo Alto Networks XDR-Analyst Exam Questions Assist You In Exam Preparation?



P2Pexam
Your Study Partner

Palo Alto Networks

XDR-Analyst

Palo Alto Networks XDR Analyst

Questions & Answers PDF

(Demo Version – Limited Content)

For More Information – Visit link below:

https://p2pexam.com/

Visit us at: https://p2pexam.com/xdr-analyst

The clients can download our products and use our XDR-Analyst study materials immediately after they pay successfully with their credit cards. Our system will send our XDR-Analyst learning prep in the form of mails to the client in 5-10 minutes after their successful payment. The mails provide the links and if only the clients click on the links they can log in our software immediately to learn our XDR-Analyst Guide materials. If there are something they can't understand, they can contact with our service and we will solve them right away.

## 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 | • 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 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. |

## Exam XDR-Analyst Registration | XDR-Analyst Mock Exam

For candidates who have little time to prepare for the exam, our XDR-Analyst exam dumps will be your best choice. With experienced professionals to edit, XDR-Analyst training materials are high-quality, they have covered most of knowledge points for the exam, if you choose, you can improve your efficiency. In addition, we have a professional team to collect and research the latest information for the XDR-Analyst Exam Materials. Free update for one year is available, and the update version for XDR-Analyst material will be sent to your email automatically.

## Palo Alto Networks XDR Analyst Sample Questions (Q62-Q67):

**NEW QUESTION # 62**
When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

- A. Delete the selected Incidents.
- B. Change the status of multiple incidents.
- C. Assign incidents to an analyst in bulk.
- D. Investigate several Incidents at once.

**Answer: B,C**

Explanation:
When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 Reference:
Assign Incidents to an Analyst in Bulk
Change the Status of Multiple Incidents

**NEW QUESTION # 63**
When using the "File Search and Destroy" feature, which of the following search hash type is supported?

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

**Answer: A**

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 # 64**
Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

- A. exception profiles that apply to specific endpoints
- B. global exception profiles that apply to all endpoints
- C. agent exception profiles that apply to specific endpoints
- D. role-based profiles that apply to specific endpoints

**Answer: B,C**

Explanation:
Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives. Reference:
Exception Security Profiles
Create an Agent Exception Profile
Create a Global Exception Profile

**NEW QUESTION # 65**
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. Lead threats can't be prevented in the future because they already exist in the environment.
- C. Build a search query using Query Builder or XQL using a list of IOCs.
- D. Create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.

**Answer: D**

Explanation:
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"

**NEW QUESTION # 66**
Which Exploit Protection Module (EPM) can be used to prevent attacks based on OS function?

- A. Memory Limit Heap Spray Check
- B. UASLR
- C. JIT Mitigation
- D. DLL Security

**Answer: C**

Explanation:

JIT Mitigation is an Exploit Protection Module (EPM) that can be used to prevent attacks based on OS function. JIT Mitigation protects against exploits that use the Just-In-Time (JIT) compiler of the OS to execute malicious code. JIT Mitigation monitors the memory pages that are allocated by the JIT compiler and blocks any attempts to execute code from those pages. This prevents attackers from using the JIT compiler as a way to bypass other security mechanisms such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Reference:
Palo Alto Networks. (2023). PCDRA Study Guide. PDF file. Retrieved from
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf Palo Alto Networks. (2021). Exploit Protection Modules. Web page. Retrieved from https://docs.paloaltonetworks.com/traps/6-0/traps-endpoint-security-manager-admin/traps-endpoint-security-policies/exploit-protection-modules.html

**NEW QUESTION # 67**
......

The procedures of buying our XDR-Analyst study materials are simple and save the clients' time. We will send our XDR-Analyst exam question in 5-10 minutes after their payment. Because the most clients may be busy in their jobs or other significant things, the time they can spare to learn our XDR-Analyst learning guide is limited and little. But if the clients buy our XDR-Analyst training quiz they can immediately use our product and save their time. And the quality of our exam dumps are very high!

**Exam XDR-Analyst Registration**: https://www.verifieddumps.com/XDR-Analyst-valid-exam-braindumps.html

- 100% Pass High-quality Palo Alto Networks - XDR-Analyst - Palo Alto Networks XDR Analyst Latest Exam Online □ Search for □ XDR-Analyst □ and easily obtain a free download on 「 www.prepawaypdf.com 」 □XDR-Analyst Authorized Exam Dumps
- Reliable XDR-Analyst Exam Registration □ XDR-Analyst Exam Cram Review □ Mock XDR-Analyst Exams □ Search for ➠ XDR-Analyst □ on ▶ www.pdfvce.com ◀ immediately to obtain a free download □Valid XDR-Analyst Exam Vce
- XDR-Analyst Learning Materials □ Practice XDR-Analyst Test Online □ Reliable XDR-Analyst Exam Registration □ Search for " XDR-Analyst " and obtain a free download on ➽ www.vceengine.com □ □Mock XDR-Analyst Exams
- Hot XDR-Analyst Latest Exam Online – The Best Exam Registration for XDR-Analyst - Efficient XDR-Analyst Mock Exam □ Search for ➤ XDR-Analyst □ and easily obtain a free download on ➠ www.pdfvce.com □ □Reliable XDR-Analyst Exam Registration
- XDR-Analyst Learning Materials □ Valid Dumps XDR-Analyst Book □ Original XDR-Analyst Questions □ Open □ www.testkingpass.com □ enter 《 XDR-Analyst 》 and obtain a free download □XDR-Analyst Exam Cram Review
- Marvelous XDR-Analyst Latest Exam Online - Unparalleled Source of XDR-Analyst Exam □ Search for 【 XDR-Analyst 】 and download it for free on 「 www.pdfvce.com 」 website □Free XDR-Analyst Vce Dumps
- XDR-Analyst Training For Exam □ XDR-Analyst Authorized Exam Dumps □ XDR-Analyst Valid Braindumps Ppt □ Copy URL ✔ www.practicevce.com □✔□ open and search for （ XDR-Analyst ） to download for free □XDR-Analyst Authorized Exam Dumps
- 100% Pass High-quality Palo Alto Networks - XDR-Analyst - Palo Alto Networks XDR Analyst Latest Exam Online □ Search for ▶ XDR-Analyst ◀ and easily obtain a free download on 【 www.pdfvce.com 】 □Free XDR-Analyst Vce Dumps
- Seeing The XDR-Analyst Latest Exam Online Means that You Have Passed Half of Palo Alto Networks XDR Analyst □ Open website □ www.torrentvce.com □ and search for 【 XDR-Analyst 】 for free download □Valid XDR-Analyst Exam Vce
- XDR-Analyst Reliable Exam Question □ XDR-Analyst Authorized Exam Dumps □ XDR-Analyst Authorized Exam Dumps □ Open ➠ www.pdfvce.com □ and search for 《 XDR-Analyst 》 to download exam materials for free □ □Exam Vce XDR-Analyst Free
- Exam XDR-Analyst Pass Guide □ Exam XDR-Analyst Pass Guide □ Exam XDR-Analyst Pass Guide □ Search for ⇒ XDR-Analyst ⇐ and download it for free immediately on □ www.prep4away.com □ □PDF XDR-Analyst VCE
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, pastebin.com, telegra.ph, 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, 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, anonup.com, www.stes.tyc.edu.tw, Disposable vapes