# 100% Pass Quiz 2026 Palo Alto Networks XDR-Analyst– High Pass-Rate Interactive EBook


BONUS!!! Download part of Actual4test XDR-Analyst dumps for free: https://drive.google.com/open?id=19D-9VmokdTumIJtk4_rqm64eoWICAU7e

The three versions of our XDR-Analyst exam questions have their own unique characteristics. The PDF version of XDR-Analyst training materials is convenient for you to print, the software version can provide practice test for you and the online version is for you to read anywhere at any time. If you are hesitating about which version should you choose, you can download our XDR-Analyst free demo first to get a firsthand experience before you make any decision. You will love our XDR-Analyst study guide for sure!

## Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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 2 | • 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 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 | • 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. |

# Latest XDR-Analyst Exam Format & XDR-Analyst Pdf Version

Even you have no basic knowledge about the XDR-Analyst study materials. You still can pass the exam with our help. The key point is that you are serious on our XDR-Analyst exam questions and not just kidding. Our XDR-Analyst practice engine can offer you the most professional guidance, which is helpful for your gaining the certificate. And our XDR-Analyst learning guide contains the most useful content and keypoints which will come up in the real exam.

# Palo Alto Networks XDR Analyst Sample Questions (Q56-Q61):

**NEW QUESTION # 56**
Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

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

**Answer: D**

Explanation:
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

**NEW QUESTION # 57**
Which statement regarding scripts in Cortex XDR is true?

- A. Any version of Python script can be run.
- B. Any script can be imported including Visual Basic (VB) scripts.
- C. The level of risk is assigned to the script upon import.
- D. The script is run on the machine uploading the script to ensure that it is operational.

**Answer: C**

Explanation:
The correct answer is B, the level of risk is assigned to the script upon import. When you import a script to the Agent Script Library in Cortex XDR, you need to specify the level of risk associated with the script. The level of risk determines the permissions and restrictions for running the script on endpoints. The levels of risk are:
Low: The script can be run on any endpoint without requiring approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.
Medium: The script can be run on any endpoint, but requires approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.
High: The script can only be run on isolated endpoints, and requires approval from the Cortex XDR administrator. The script cannot be used in remediation suggestions or automation actions.
The other options are incorrect for the following reasons:
A is incorrect because not any version of Python script can be run in Cortex XDR. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. For example, the scripts must not exceed 64 KB in size, must not use external libraries or modules, and must not contain malicious or harmful code.

C is incorrect because not any script can be imported to Cortex XDR, including Visual Basic (VB) scripts. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. VB scripts are not supported by Cortex XDR, and will not run on the endpoints.
D is incorrect because the script is not run on the machine uploading the script to ensure that it is operational. The script is only validated for syntax errors and size limitations when it is imported to the Agent Script Library. The script is not executed or tested on the machine uploading the script, and the script may still fail or cause errors when it is run on the endpoints.
Reference:
Agent Script Library
Import a Script
Run Scripts on an Endpoint

**NEW QUESTION # 58**
Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

- A. Quarantine
- B. Isolation
- C. Search & destroy
- D. Flag for removal

**Answer: A**

Explanation:
The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console. Reference:
Quarantine Files
Manage Quarantined Files

**NEW QUESTION # 59**
Where would you view the WildFire report in an incident?

- A. next to relevant Key Artifacts in the incidents details page
- B. on the HUB page at apps.paloaltonetworks.com
- C. under Response --> Action Center
- D. under the gear icon --> Agent Audit Logs

**Answer: A**

Explanation:
To view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. A key artifact is a piece of evidence that is associated with an alert or an incident, such as a file hash, a registry key, an IP address, a domain name, or a full path. If a key artifact is related to a WildFire analysis, you will see a WildFire icon next to it, indicating that there is a WildFire report available for that artifact. You can click on the WildFire icon to view the report, which will show you the detailed information about the artifact, such as the verdict, the behavior, the severity, the signatures, and the screenshots12.
Let's briefly discuss the other options to provide a comprehensive explanation:
B . under Response --> Action Center: This is not the correct answer. The Action Center is a feature 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 does not show you the WildFire reports for the incidents, but it can help you to remediate the incidents by applying the appropriate actions3.
C . under the gear icon --> Agent Audit Logs: This is not the correct answer. The Agent Audit Logs are logs that show you the activities and events that occurred on the Cortex XDR agents, such as installation, upgrade, connection, policy update, or prevention. The Agent Audit Logs do not show you the WildFire reports for the incidents, but they can help you to troubleshoot the agent issues or verify the agent status4.

D . on the HUB page at apps.paloaltonetworks.com: This is not the correct answer. The HUB page is a web portal that allows you to access and manage your Palo Alto Networks applications, such as Cortex XDR, Cortex XSOAR, Prisma Cloud, or AutoFocus. The HUB page does not show you the WildFire reports for the incidents, but it can help you to navigate to the different applications or view the notifications and alerts5.
In conclusion, to view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. By viewing the WildFire report, you can gain more insights and context about the incident and the artifact.
Reference:
View Incident Details
View WildFire Reports
Action Center
Agent Audit Logs
HUB

**NEW QUESTION # 60**
Cortex XDR is deployed in the enterprise and you notice a cobalt strike attack via an ongoing supply chain compromise was prevented on 1 server. What steps can you take to ensure the same protection is extended to all your servers?

- A. Enable DLL Protection on all servers but there might be some false positives.
- B. Create IOCs of the malicious files you have found to prevent their execution.
- C. Conduct a thorough Endpoint Malware scan.
- D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

**Answer: B**

Explanation:
The best step to ensure the same protection is extended to all your servers is to create indicators of compromise (IOCs) of the malicious files you have found to prevent their execution. IOCs are pieces of information that indicate a potential threat or compromise on an endpoint, such as file hashes, IP addresses, domain names, or registry keys. You can create IOCs in Cortex XDR to block or alert on any file or network activity that matches the IOCs. By creating IOCs of the malicious files involved in the cobalt strike attack, you can prevent them from running or spreading on any of your servers.
The other options are not the best steps for the following reasons:
A is not the best step because conducting a thorough Endpoint Malware scan may not detect or prevent the cobalt strike attack if the malicious files are obfuscated, encrypted, or hidden. Endpoint Malware scan is a feature of Cortex XDR that allows you to scan endpoints for known malware and quarantine any malicious files found. However, Endpoint Malware scan may not be effective against unknown or advanced threats that use evasion techniques to avoid detection.
B is not the best step because enabling DLL Protection on all servers may cause some false positives and disrupt legitimate applications. DLL Protection is a feature of Cortex XDR that allows you to block or alert on any DLL loading activity that matches certain criteria, such as unsigned DLLs, DLLs loaded from network locations, or DLLs loaded by specific processes. However, DLL Protection may also block or alert on benign DLL loading activity that is part of normal system or application operations, resulting in false positives and performance issues.
C is not the best step because enabling Behavioral Threat Protection (BTP) with cytool may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection. Behavioral Threat Protection is a feature of Cortex XDR that allows you to block or alert on any endpoint behavior that matches certain patterns, such as ransomware, credential theft, or lateral movement. Cytool is a command-line tool that allows you to configure and manage the Cortex XDR agent on the endpoint. However, Behavioral Threat Protection may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection, such as encryption, obfuscation, or proxy servers.
Reference:
Create IOCs
Scan an Endpoint for Malware
DLL Protection
Behavioral Threat Protection
Cytool for Windows

**NEW QUESTION # 61**
.....

God always helps those who help themselves. It is impossible to make great fortune overnight. Enough preparation and efforts are needed when you come across an opportunity. So we suggest that you learn our XDR-Analyst latest training material, which can help broaden your knowledge. Nowadays, lifelong learning has got wide attention. The much knowledge you learn, the better chance you will have. Our XDR-Analyst practice material suits you best. You can elevate your ability in a short time. Then you can apply what you have learned on our XDR-Analyst test engine into practice. We warmly welcome you to purchase our study guide.

**Latest XDR-Analyst Exam Format**: https://www.actual4test.com/XDR-Analyst_examcollection.html

- XDR-Analyst Reliable Test Bootcamp □ XDR-Analyst Mock Exams □ XDR-Analyst Valid Test Sims □ Simply search for { XDR-Analyst } for free download on □ www.verifieddumps.com □ □XDR-Analyst Training Tools
- Real Palo Alto Networks XDR-Analyst Exam Questions in PDF Format □ 「 www.pdfvce.com 」 is best website to obtain ➽ XDR-Analyst □ for free download □XDR-Analyst Latest Real Exam
- XDR-Analyst dumps materials - exam dumps for XDR-Analyst: Palo Alto Networks XDR Analyst ✈ Copy URL （ www.practicevce.com ） open and search for □ XDR-Analyst □ to download for free □XDR-Analyst Pdf Torrent
- New XDR-Analyst Test Experience □ XDR-Analyst Valid Exam Pdf □ XDR-Analyst Training Tools □ Search for ▹ XDR-Analyst ◃ on ▹ www.pdfvce.com ◃ immediately to obtain a free download □XDR-Analyst New Braindumps Files
- Test XDR-Analyst Collection □ XDR-Analyst Valid Exam Pdf □ Dumps XDR-Analyst Torrent □ Search for ⇛ XDR-Analyst ⇚ and obtain a free download on ➤ www.exam4labs.com □ □XDR-Analyst Latest Real Exam
- XDR-Analyst Trusted Exam Resource □ XDR-Analyst New Braindumps Files □ XDR-Analyst Pdf Torrent □ Search for 「 XDR-Analyst 」 and download it for free immediately on ✔ www.pdfvce.com □✔□ □XDR-Analyst Mock Exams
- XDR-Analyst dumps materials - exam dumps for XDR-Analyst: Palo Alto Networks XDR Analyst □ Download 【 XDR-Analyst 】 for free by simply searching on （ www.exam4labs.com ） □XDR-Analyst New Braindumps Files
- XDR-Analyst Trusted Exam Resource □ Test XDR-Analyst Collection □ Study Guide XDR-Analyst Pdf □ Simply search for ▸ XDR-Analyst ◂ for free download on □ www.pdfvce.com □ □XDR-Analyst Valid Exam Pdf
- XDR-Analyst dumps materials - exam dumps for XDR-Analyst: Palo Alto Networks XDR Analyst ✴ Search for [ XDR-Analyst ] on □ www.examdiscuss.com □ immediately to obtain a free download □New XDR-Analyst Exam Answers
- Real Palo Alto Networks XDR-Analyst Exam Questions in PDF Format □ The page for free download of 【 XDR-Analyst 】 on ⇛ www.pdfvce.com ⇚ will open immediately □XDR-Analyst Pdf Torrent
- XDR-Analyst Associate Level Exam □ Reliable Exam XDR-Analyst Pass4sure □ XDR-Analyst Associate Level Exam □ Open website 「 www.pdfdumps.com 」 and search for ▸ XDR-Analyst ◂ for free download □XDR-Analyst New Braindumps Files
- deweypkwo317934.mysticwiki.com, zbookmarkhub.com, lexieihpn561861.corpfinwiki.com, marcrnjd326734.slypage.com, leantheprocess.com, lillijhsh302738.gynoblog.com, haseebjhfs972234.blog2news.com, janasfye231133.newsbloger.com, mayagexd500250.luwebs.com, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of Actual4test XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=19D-9VmokdTumIJtk4_rqm64eoWICAU7e