
# PALO ALTO XDR-ENGINEER

## Palo Alto XDR-Engineer Certification Questions & Answers

Exam Summary – Syllabus – Questions

**XDR-ENGINEER**

**Palo Alto Networks Certified XDR Engineer**

**50 Questions Exam – 860 on a scale of 300 to 1000 Cut Score – Duration of 90 minutes**

## Table of Contents:

# Know Your XDR-Engineer Certification Well:

The XDR-Engineer is best suitable for candidates who want to gain knowledge in the Palo Alto Security Operations. Before you start your XDR-Engineer preparation you may struggle to get all the crucial XDR-Engineer materials like XDR-Engineer syllabus, sample questions, study guide.

But don't worry the XDR-Engineer PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the XDR-Engineer syllabus?
- How many questions are there in the XDR-Engineer exam?
- Which Practice test would help me to pass the XDR-Engineer exam at the first attempt?

Passing the XDR-Engineer exam makes you Palo Alto Networks Certified XDR Engineer. Having the XDR-Engineer certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

# Palo Alto XDR-Engineer Certification Details:

| | |
|---|---|
| **Exam Name** | Palo Alto Networks XDR Engineer |
| **Exam Code** | XDR-Engineer |
| **Exam Price** | $250 USD |
| **Duration** | 90 minutes |
| **Number of Questions** | 50 |
| **Passing Score** | 860 on a scale of 300 to 1000 |
| **Recommended Training** | **Cortex XDR: Security Operations and Integration** |
| **Exam Registration** | **PEARSON VUE** |
| **Sample Questions** | **Palo Alto XDR-Engineer Sample Questions** |
| **Practice Exam** | **Palo Alto Networks Certified XDR Engineer Practice Test** |

# XDR-Engineer Syllabus:

| Section | Weight | Objectives |
|---|---|---|
| Planning and Installation | 14% | - Explain the deployment process, objectives, and resources (e.g., hardware, software, data sources, integrations)<br>- Explain the deployment and functionality of Cortex XDR components<br>• XDR agent<br>• Broker VM<br>• XDR Collector<br>• Cloud Identity Engine<br>- Configure user roles, permissions, and access controls<br>- Demonstrate understanding of data retention and compute units |
| Cortex XDR Agent Configuration | 22% | - Configure endpoint prevention profiles and policies<br>- Configure endpoint extension profiles and policies<br>- Configure endpoint groups |
| Ingestion and Automation | 22% | - Onboard data sources (e.g., NGFW, network, cloud, identity)<br>- Manage simple automation rules<br>- Configure Broker VM applets and clusters<br>- Configure XDR Collectors<br>- Configure parsing rules |
| Detection and Reporting | 22% | - Create detection rules to align with requirements<br>• Correlation<br>• Custom prevention rules<br>• Behavioral indicators of compromise (BIOCs) and indicators of compromise (IOCs)<br>- Configure exceptions and exclusions<br>- Create custom dashboards and reporting templates |
| Maintenance and Troubleshooting | 20% | - Manage Cortex XDR software component updates (e.g., content, agents, Collectors, Broker VM)<br>- Troubleshoot data management issues (e.g., data |

| Section | Weight | Objectives |
|---|---|---|
| | | ingestion, parsing)<br>- Troubleshoot Cortex XDR components (e.g., agents, Collectors, Broker VM) |

# Palo Alto XDR-Engineer Sample Questions:

Question: 1

Which two capabilities does the Host Firewall extension provide? (Choose two)

a) Application-level packet filtering
b) URL blocking
c) IP-based traffic control
d) Endpoint group filtering

**Answer: a, c**

Question: 2

What are two benefits of correlating multiple alert types into a single detection rule? (Choose two)

a) Easier alert suppression
b) Improved root cause analysis
c) Reduced rule licensing cost
d) Higher fidelity detections

**Answer: b, d**

Question: 3

Where can you monitor alert volume trends from detection rules over the past 30 days?

(Choose two)

a) Dashboard#
b) Detection Rules Metrics tab
c) Agent Profile page
d) Incidents Overview

**Answer: a, b**

Question: 4

During deployment planning, what is a critical prerequisite to install and activate the XDR Broker VM?

a) An active NGFW device
b) A signed endpoint license file
c) A static MAC address reservation for XDR Collector
d) A registered Broker VM token from Cortex XDR

**Answer: d**

Question: 5

Who benefits the most from automated dashboard reports? (Choose two)

a) Security engineers
b) External auditors
c) Development team
d) SOC managers

**Answer: a, d**

Question: 6

Cortex XDR provides data retention tied to Compute Units (CUs). What does the CU determine?

a) Number of endpoints that can be monitored
b) Duration of historical data available for queries
c) Number of detection rules allowed
d) The level of user access privileges

**Answer: b**

Question: 7

When creating an extension profile, what "whitelisting" feature allows known safe scripts to bypass behavioral restrictions?

a) Global exclusions
b) Trusted Signer Exceptions
c) Behavioral Allow List
d) IOC Exceptions

**Answer: c**

Question: 8

Why might an endpoint show as “Disconnected” in Cortex XDR even if the operating system is functioning normally?

a) The agent service is not running or is blocked by local firewall
b) The agent is using an outdated policy
c) The host is not part of the trusted domain
d) The endpoint has been offboarded

**Answer: a**

Question: 9

What would be the best way to apply different security policies to Linux and Windows endpoints using Cortex XDR?

a) Create separate user roles
b) Use external scripts to apply policies
c) Manually assign each policy to every agent
d) Use OS filters in endpoint groups

**Answer: d**

Question: 10

Which component is responsible for interpreting custom log formats in Cortex XDR?

a) Behavioral analytics engine
b) Parsing rule editor
c) Policy management module
d) IOC management engine

**Answer: b**

# Study Guide to Crack Palo Alto XDR-Engineer Exam:

- Getting details of the XDR-Engineer syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the XDR-Engineer exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.

- Joining the Palo Alto provided training for XDR-Engineer exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the XDR-Engineer sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on XDR-Engineer practice tests is must. Continuous practice will make you an expert in all syllabus areas.