PALO ALTO PCDRA

Palo Alto Detection and Remediation Analyst Certification Questions & Answers

Exam Summary – Syllabus – Questions

PCDRA

[Palo Alto Networks Certified Detection and Remediation Analyst]

60-75 Questions Exam – Variable (70-80 / 100 Approx.) Cut Score – Duration of 80 minutes

Table of Contents:

Know Your PCDRA Certification Well:

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

But don't worry the PCDRA 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 PCDRA syllabus?
- How many questions are there in the PCDRA exam?
- Which Practice test would help me to pass the PCDRA exam at the first attempt?

Passing the PCDRA exam makes you Palo Alto Networks Certified Detection and Remediation Analyst. Having the Detection and Remediation Analyst 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 PCDRA Detection and Remediation Analyst Certification Details:

Exam Name	Detection and Remediation Analyst
Exam Code	PCDRA
Exam Price	$155 USD
Duration	80 minutes
Number of Questions	60-75
Passing Score	Variable (70-80 / 100 Approx.)
Recommended Training	**Cortex XDR 2: Prevention, Analysis, and Response (EDU 260)** **Digital Learning - Cortex XDR** **PCDRA Study Guide**
Exam Registration	**PEARSON VUE**

Sample Questions	**Palo Alto PCDRA Sample Questions**
Practice Exam	**Palo Alto Networks Certified Detection and Remediation Analyst Practice Test**

PCDRA Syllabus:

Section	**Objectives**
Threats and Attacks 10%	
Recognize the different types of attacks	- Differentiate between exploits and malware. - Define a file-less attack. - Define a supply chain attack. - Outline ransomware threats.
Recognize common attack tactics	- List common attack tactics - Define various attack tactics. - Outline MITRE framework steps.
Recognize various types of threats/vulnerabilities	- Differentiate between threats and attacks. - Define product modules that help identify threats. - Identify legitimate threats (true positives) vs. illegitimate threats (false positives). - Summarize the generally available references for vulnerabilities.
Prevention and Detection 20%	
Recognize common defense systems	- Identify ransomware defense systems. - Summarize device management defenses.
Identify attack vectors.	- Summarize how to prevent agent attacks. - Describe how to use XDR to prevent supply chain attacks. - Describe how to use XDR to prevent phishing attacks. - Characterize the differences between malware and exploits. - Categorize the types and structures of vulnerabilities.
Outline malware prevention.	- Define behavioral threat protection. - Identify the profiles that must be configured for malware prevention.

Section	Objectives
	- Outline malware protection flow. - Describe the uses of hashes in Cortex XDR. - Identify the use of malware prevention modules (MPMs).
Outline exploit prevention	- Identify the use of exploit prevention modules (EPMs). - Define default protected processes. - Characterize the differences between application protection and kernel protection.
Outline analytic detection capabilities	- Define the purpose of detectors. - Define machine learning in the context of analytic detection. - Identify the connection of analytic detection capabilities to MITRE.
Investigation 20%	
Identify the investigation capabilities of Cortex XDR	- Describe how to navigate the console. - Identify the remote terminal options. - Characterize the differences between incidents and alerts. - Characterize the differences between exclusions and exceptions.
Identify the steps of an investigation	- Clarify how incidents and alerts interrelate. - Identify the order in which to resolve incidents. - Identify which steps are valid for an investigation. - List the options to highlight or suppress incidents.
Identify actions to investigate incidents	- Describe when to perform actions using the live terminal. - Describe what actions can be performed using the live terminal. - Describe when to perform actions using a script. - Identify common investigation screens and processes.

Section	Objectives
Outline incident collaboration and management using XDR.	- Outline, read, and write attributes. - Characterize the difference between incidents and alerts.
Remediation 15%	
Describe basic remediation	- Describe how to navigate the remediation suggestions. - Distinguish between automatic vs. manual remediations. - Summarize how/when to run a script. - Describe how to fix false positives.
Define examples of remediation	- Define ransomware. - Define registry. - Define file changes/deletions.
Define configuration options in XDR to fix problems	- Define blocklist. - Define signers. - Define allowlist. - Define exceptions. - Define quarantine/isolation. - Define file search and destroy.
Threat Hunting 10%	
Outline the tools for threat hunting	- Explain the purpose and use of the IOC technique. - Explain the purpose and use of the BIOC technique. - Explain the purpose and use of the XQL technique. - Explain the purpose and use of the query builder technique.
Identify how to prevent the threat	- Convert BIOCs into custom prevention rules.
Manage threat hunting	- Describe the purpose of Unit 42.
Reporting 10%	
Identify the reporting capabilities of XDR	- Leverage reporting tools.
Outline how to build a quality report	- Identify what is relevant to a report given context.

Section	Objectives
	- Interpret meaning from a report. - Identify the information needed for a given audience. - Outline the capabilities of XQL to build a report. - Outline distributing and scheduling capabilities of Cortex XDR.
Architecture 15%	
Outline components of Cortex XDR	- Define the role of Cortex XDR Data Lake. - Define the role of Cortex Agent. - Define the role of Cortex Console. - Define the role of Cortex Broker. - Distinguish between different proxies. - Define the role of Directory Sync. - Define the role of Wildfire.
Describe communication among components	- Define communication of data lakes. - Define communication for Wildfire. - Define communication options/channels to and from the client. - Define communication for external dynamic list (EDL). - Define communication from the broker.
Describe the architecture of agent related to different operating systems	- Recognize different supported operating systems. - Characterize the differences between functions or features on operating systems.
Outline how Cortex XDR ingests other non-Palo Alto Networks data sources.	- Outline all ingestion possibilities. - Describe details of the ingestion methods.
Overview of functions and deployment of Broker	- Outline deployment of Broker. - Describe how to use the Broker to ingest third party alert. - Describe how to use the Broker as a proxy between the agents and XDR in the Cloud. - Describe how to use the Broker to activate Pathfinder.

Palo Alto PCDRA Sample Questions:

Question: 1

You notice that a hardware device is damaged and important data files have been completely erased from the system. What kind of threat appears to be present here?

a) Interruption
b) Interception
c) Fabrication
d) Modification

Answer: a

Question: 2

What is the expiration limit set by Cortex XDR by default for agent upgradation and agent uninstall?

a) 90 days
b) 60 days
c) 40 days
d) 30 days

Answer: d

Question: 3

How does an attacker prefer to carry out supply-chain attacks?

a) By targeting an organization directly through phishing or exploitation of vulnerabilities
b) By targeting employees (software developers) of the target organization
c) By targeting items that aren’t written to disk
d) By targeting an organization's upper management directly

Answer: b

Question: 4

How much RAM is required in Cortex XDR agent 7.2 for Windows?

a) 2GB minimum
b) 4GB; 8GB recommended
c) 3GB minimum
d) 512MB minimum; 2GB recommended

Answer: a

Question: 5

Cortex XDR automatically disables BIOC rules that reach how many hits over what period of time?

a) 5,000 or more hits over a 24-hour period
b) 1,000 or more hits over a 24-hour period
c) 5,000 or more hits over a 12-hour period
d) 1,000 or more hits over a 12-hour period

Answer: a

Question: 6

The Action Center can be found on which tab?

a) Reporting
b) Investigation
c) Response
d) Endpoints

Answer: c

Question: 7

What does the term “TCP/IP” stand for?

a) Transmission Contribution Protocol/ internet protocol
b) Transmission Control Protocol/ internet protocol
c) Transaction Control Protocol/ internet protocol
d) Transmission Control Prevention/ internet protocol

Answer: b

Question: 8

The Response action breakdown widget belongs to which of the following widget categories?

a) Agent Management Widgets
b) Incident Management Widgets
c) Investigation Widgets
d) User Defined Widgets

Answer: c

Question: 9

Which of the following is a summary of the remediation suggestions to apply to the file or registry?

a) Suggested remediation
b) Original event description
c) Remediation status
d) Suggested remediation description

Answer: d

Question: 10

The analytics engine creates and maintains a very large number of profile types, but they can all be categorized into how many categories in general?

a) 4
b) 2
c) 3
d) 5

Answer: c

Study Guide to Crack Palo Alto Detection and Remediation Analyst PCDRA Exam:

- Getting details of the PCDRA 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 PCDRA 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 PCDRA 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 PCDRA 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 PCDRA practice tests is must. Continuous practice will make you an expert in all syllabus areas.