



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.



PCDRA MCQs
PCDRA TestPrep
PCDRA Study Guide
PCDRA Practice Test
PCDRA Exam Questions



Palo-Alto

PCDRA

Palo Alto Networks Certified Detection and Remediation Analyst



<https://killexams.com/pass4sure/exam-detail/PCDRA>

Question: 226

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion .

What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

- A. mark the incident as Unresolved
- B. create a BIOC rule excluding this behavior
- C. create an exception to prevent future false positives
- D. mark the incident as Resolved C False Positive

Answer: D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/alert-exclusions/add-an-alert-exclusion.html>

Question: 227

To create a BIOC rule with XQL query you must at a minimum filter on which field in order for it to be a valid BIOC rule?

- A. causality_chain
- B. endpoint_name
- C. threat_event
- D. event_type

Answer: D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-bioc-rule.html>

Question: 228

After scan, how does file quarantine function work on an endpoint?

- A. Quarantine takes ownership of the files and folders and prevents execution through access control.
- B. Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.
- C. Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.
- D. Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XD

Answer: C

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/investigation-and-response/investigate-files/manage-quarantined-files>

Question: 229

Which statement is true for Application Exploits and Kernel Exploits?

- A. The ultimate goal of any exploit is to reach the application.
- B. Kernel exploits are easier to prevent than application exploits.
- C. The ultimate goal of any exploit is to reach the kernel.
- D. Application exploits leverage kernel vulnerability.

Answer: A

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/about-cortex-xdr-protection.html>

Question: 230

Which of the following best defines the Windows Registry as used by the Cortex XDRagent?

- A. a hierarchical database that stores settings for the operating system and for applications
- B. a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the âswapâ
- C. a central system, available via the internet, for registering officially licensed versions of software to prove ownership
- D. a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>

Question: 231

What kind of the threat typically encrypts userfiles?

- A. ransomware
- B. SQL injection attacks
- C. Zero-day exploits
- D. supply-chain attacks

Answer: A

Explanation:

Reference: <https://www.proofpoint.com/us/threat-reference/ransomware#:~:text=Ransomware%20is%20a%20type%20of,ransom%20fee%20to%20the%20attacker>

Question: 232

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate .

Which statement is correct for the incident?

- A. It is true positive.
- B. It is false positive.
- C. It is a false negative.
- D. It is true negative.

Answer: B

Explanation:

Reference: <https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/cortex-xdr-false-positive-cloud2model-manager-1-005/td-p/391391>

Question: 233

LiveTerminal uses which type of protocol to communicate with the agent on the endpoint?

- A. NetBIOS over TCP
- B. WebSocket
- C. UDP and a random port
- D. TCP, over port 80

Answer: B

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/communication-between-cortex-xdr-and-agents.html>

Question: 234

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically close the connections involved in malicious traffic.
- B. Automatically kill the processes involved in malicious activity.
- C. Automatically terminate the threads involved in malicious activity.
- D. Automatically block the IP addresses involved in malicious traffic.

Answer: A,D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-security-profiles/add-malware-security-profile.html#:~:text=With%20Behavioral%20threat%20protection%2C%20the,appear%20legitimate%20if%20inspected%20individually>

Question: 235

Which of the following policy exceptions applies to the following description?

âAn exception allowing specific PHP filesâ

- A. Support exception
- B. Local file threat examination exception
- C. Behavioral threat protection rule exception
- D. Process exception

Answer: B

Question: 236

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

- A. Security Manager Dashboard
- B. Data Ingestion Dashboard
- C. Security Admin Dashboard
- D. Incident Management Dashboard

Answer: A

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/release-information/features-introduced/features-introduced-in-2021.html>

Question: 237

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

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

Answer: A,B

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/release-information/features-introduced/features-introduced-in-2021.html>

Question: 238

Which of the following represents the correct relation of alerts to incidents?

- A. Only alerts with the same host are grouped together into one Incident in a given time frame.
- B. Alerts that occur within a three hour time frame are grouped together into one Incident.
- C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
- D. Every alert creates a new Incident.

Answer: A

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-incidents/cortex-xdr-incidents.html>

Question: 239

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

- A. Broker VM Pathfinder
- B. Local Agent Proxy
- C. Local Agent Installer and Content Caching
- D. Broker VM Syslog Collector

Answer: C

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/broker-vm/set-up-broker-vm/activate-the-agent-proxy-for-closed-networks.html>

Question: 240

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

- A. Click the three dots on the widget and then choose "Save" and this will link the query to the Widget Library.
- B. This isn't supported, you have to exit the dashboard and go into the Widget Library first to create it.
- C. Click on "Save to Action Center" in the dashboard and you will be prompted to give the query a name and description.
- D. Click on "Save to Widget Library" in the dashboard and you will be prompted to give the query a name and description.

Answer: D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/monitoring/cortex-xdr-dashboard/widget-library.html>

Question: 241

Phishing belongs which of the following MITRE ATT&CK tactics?

- A. Initial Access, Persistence
- B. Persistence, Command and Control
- C. Reconnaissance, Persistence
- D. Reconnaissance, Initial Access

Answer: D

Question: 242

When creating a BIOC rule, which XQL query can be used?

- A. dataset = xdr_data
| filter event_sub_type = PROCESS_START and
action_process_image_name =~ ".*?.(?:pdf|docx).exe"
- B. dataset = xdr_data
| filter event_type = PROCESS and
event_sub_type = PROCESS_START and
action_process_image_name =~ ".*?.(?:pdf|docx).exe"
- C. dataset = xdr_data
| filter action_process_image_name =~ ".*?.(?:pdf|docx).exe"
| fields action_process_image
- D. dataset = xdr_data
| filter event_behavior = true
event_sub_type = PROCESS_START and
action_process_image_name =~ ".*?.(?:pdf|docx).exe"

Answer: B

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-bioc-rule.html>

Question: 242

When creating a scheduled report which is not an option?

- A. Run weekly on a certain day and time.
- B. Run quarterly on a certain day and time.
- C. Run monthly on a certain day and time.
- D. Run daily at a certain time (selectable hours and minutes).

Answer: B

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/monitoring/cortex-xdr-dashboard/run-or-schedule-reports.html>

Question: 243

When using the "File Search and Destroy" feature, which of the following search hash type is supported?

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

Answer: A

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/response->

Question: 244

Which statement best describes how Behavioral Threat Protection (BTP) works?

- A. BTP injects into known vulnerable processes to detect malicious activity.
- B. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.
- C. BTP matches EDR data with rules provided by Cortex XD
- D. BTP uses machine Learning to recognize malicious activity even if it is not known.

Answer: A

Explanation:

Reference: <https://www.khipu-networks.com/matchmadein/wp-content/uploads/cortex-xdr- endpoint-protection-solution-guide.pdf>

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.