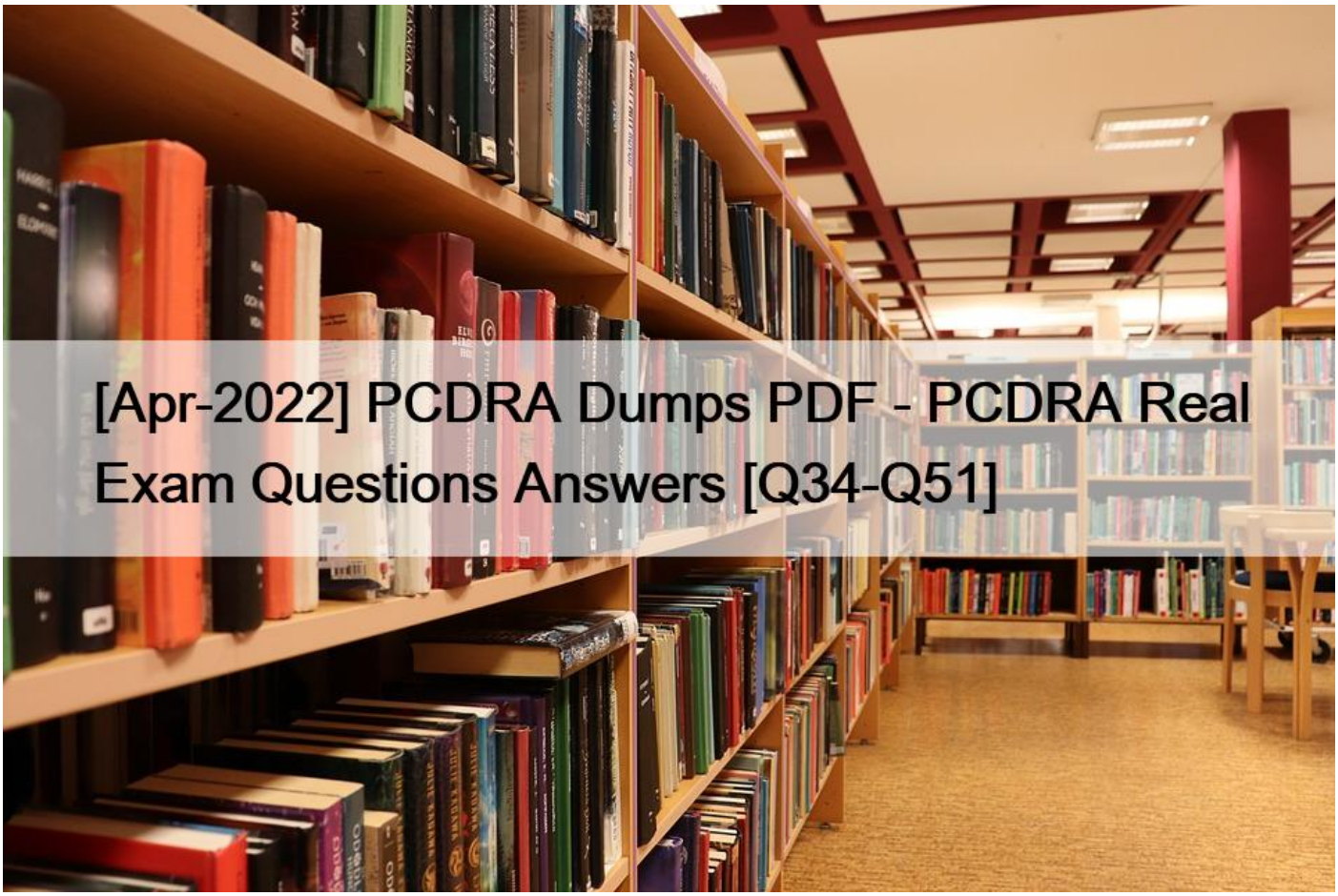
[Apr-2022 PCDRA Dumps PDF - PCDRA Real Exam Questions Answers [Q34-Q51



[Apr-2022] PCDRA Dumps PDF - PCDRA Real Exam Questions Answers
PCDRA Dumps 100% Pass Guarantee With Latest Demo

Palo Alto Networks PCDRA Exam Syllabus Topics:

TopicDetailsTopic 1- Describe how to use the Broker as a proxy between the agents and XDR in the Cloud- Describe details of the ingestion methodsTopic 2- Identify the connection of analytic detection capabilities to MITRE- List the options to highlight or suppress incidentsTopic 3- Outline how Cortex XDR ingests other non-Palo Alto Networks data sources- Describe how to use the Broker to activate PathfinderTopic 4- Identify common investigation screens and processes- Describe what actions can be performed using the live terminalTopic 5- Identify legitimate threats (true positives) vs. illegitimate threats (false positives)- Outline incident collaboration and management using XDRTopic 6- Characterize the differences between incidents and alerts- Identify the investigation capabilities of Cortex XDRTopic 7- Define communication options- channels to and from the client- Distinguish between different proxiesTopic 8- Describe how to use XDR to prevent supply chain attacks- Categorize the types and structures of vulnerabilitiesTopic 9- Outline distributing and scheduling capabilities of Cortex XDR- Identify the information needed for a given audienceTopic 10- Define product modules that help identify threats- Summarize the generally available references for vulnerabilitiesTopic 11- Distinguish between automatic vs. manual remediations- Describe how to fix false positives- Describe basic remediationTopic 12- Characterize the differences between application protection and kernel protection- Characterize the differences between malware and exploitsTopic 13-

Identify the use of malware prevention modules (MPMs)- Identify the profiles that must be configured for malware preventionTopic 14- Explain the purpose and use of the query builder technique- Explain the purpose and use of the IOC technique

NO.34 With a Cortex XDR Prevent license, which objects are considered to be sensors?
* Syslog servers
* Third-Party security devices
* Cortex XDR agents
* Palo Alto Networks Next-Generation Firewalls

NO.35 As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?
* Enable DLL Protection on all endpoints but there might be some false positives.
* Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
* No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.
* No step is required because the malicious document is already stopped.

NO.36 What is the outcome of creating and implementing an alert exclusion?
* The Cortex XDR agent will allow the process that was blocked to run on the endpoint.
* The Cortex XDR console will hide those alerts.
* The Cortex XDR agent will not create an alert for this event in the future.
* The Cortex XDR console will delete those alerts and block ingestion of them in the future.

NO.37 What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?
* Netflow Collector
* Syslog Collector
* DB Collector
* Pathfinder

NO.38 Which of the following is an example of a successful exploit?
* connecting unknown media to an endpoint that copied malware due to Autorun.
* a user executing code which takes advantage of a vulnerability on a local service.
* identifying vulnerable services on a server.
* executing a process executable for well-known and signed software.

NO.39 What license would be required for ingesting external logs from various vendors?
* Cortex XDR Pro per Endpoint
* Cortex XDR Vendor Agnostic Pro
* Cortex XDR Pro per TB
* Cortex XDR Cloud per Host

NO.40 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?
* mark the incident as Unresolved
* create a BIOC rule excluding this behavior
* create an exception to prevent future false positives

* mark the incident as Resolved – False Positive

NO.41 Which two types of exception profiles you can create in Cortex XDR? (Choose two.)
* exception profiles that apply to specific endpoints
* agent exception profiles that apply to specific endpoints
* global exception profiles that apply to all endpoints
* role-based profiles that apply to specific endpoints

NO.42 Network attacks follow predictable patterns. If you interfere with any portion of this pattern, the attack will be neutralized. Which of the following statements is correct?
* Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.
* Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.
* Cortex XDR Analytics does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.
* Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

NO.43 When is the wss (WebSocket Secure) protocol used?
* when the Cortex XDR agent downloads new security content
* when the Cortex XDR agent uploads alert data
* when the Cortex XDR agent connects to WildFire to upload files for analysis
* when the Cortex XDR agent establishes a bidirectional communication channel

NO.44 Which Type of IOC can you define in Cortex XDR?
* destination port
* e-mail address
* full path
* App-ID

NO.45 Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?
* in the macOS Malware Protection Profile to indicate allowed signers
* in the Linux Malware Protection Profile to indicate allowed Java libraries
* SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles
* in the Windows Malware Protection Profile to indicate allowed executables

NO.46 Which of the following represents the correct relation of alerts to incidents?
* Only alerts with the same host are grouped together into one Incident in a given time frame.
* Alerts that occur within a three hour time frame are grouped together into one Incident.
* Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
* Every alert creates a new Incident.

NO.47 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?
* Broker VM Pathfinder
* Local Agent Proxy
* Local Agent Installer and Content Caching
* Broker VM Syslog Collector

NO.48 When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)
* Assign incidents to an analyst in bulk.

* Change the status of multiple incidents.
* Investigate several Incidents at once.
* Delete the selected Incidents.

NO.49 When creating a BIOC rule, which XQL query can be used?
* dataset = xdr_data

| filter event_sub_type = PROCESS_START and

action_process_image_name ~= “.*?.(?:pdf|docx).exe”
* dataset = xdr_data

| filter event_type = PROCESS and

event_sub_type = PROCESS_START and

action_process_image_name ~= “.*?.(?:pdf|docx).exe”
* dataset = xdr_data

| filter action_process_image_name ~= “.*?.(?:pdf|docx).exe”

| fields action_process_image
* dataset = xdr_data

| filter event_behavior = true

event_sub_type = PROCESS_START and

action_process_image_name ~= “.*?.(?:pdf|docx).exe”

NO.50 Which module provides the best visibility to view vulnerabilities?
* Live Terminal module
* Device Control Violations module
* Host Insights module
* Forensics module

Host Insights, an add-on module for Cortex XDR, combines vulnerability assessment, application and system visibility, and a powerful Search and Destroy feature to help you identify and contain threats. Vulnerability Assessment provides you real-time visibility into vulnerability exposure and current patch levels across your end-points. Host inventory presents detailed information about your host applications and settings whileSearch and Destroy lets you swiftly find and eradicate threats across all endpoints. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce your exposure to threats so you can avoid future breached.

NO.51 As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?
* Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
* Enable DLL Protection on all servers but there might be some false positives.
* Create IOCs of the malicious files you have found to prevent their execution.
* Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

Dumps Real Palo Alto Networks PCDRA Exam Questions [Updated 2022:
https://www.examslabs.com/Palo-Alto-Networks/Palo-Alto-Certifications-and-Accreditations/best-PCDRA-exam-dumps.html]