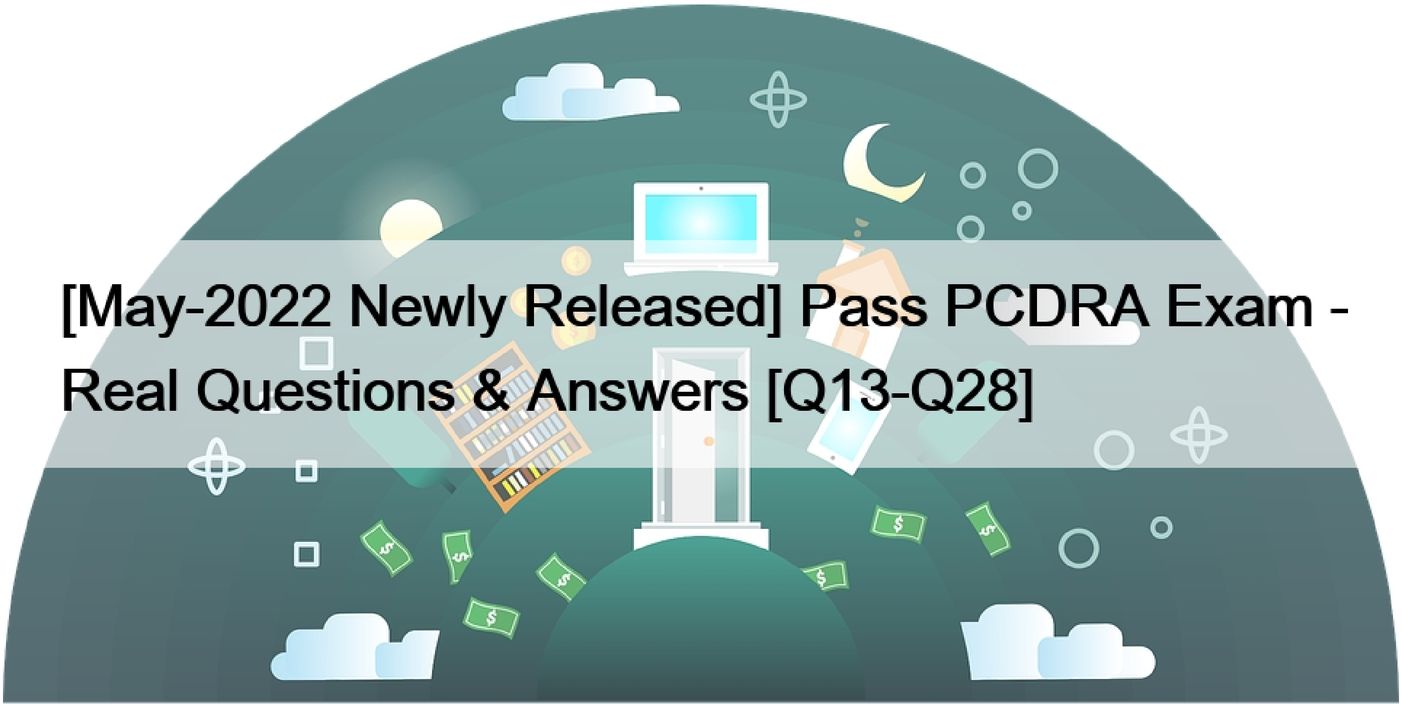
[May-2022 Newly Released Pass PCDRA Exam - Real Questions & Answers [Q13-Q28

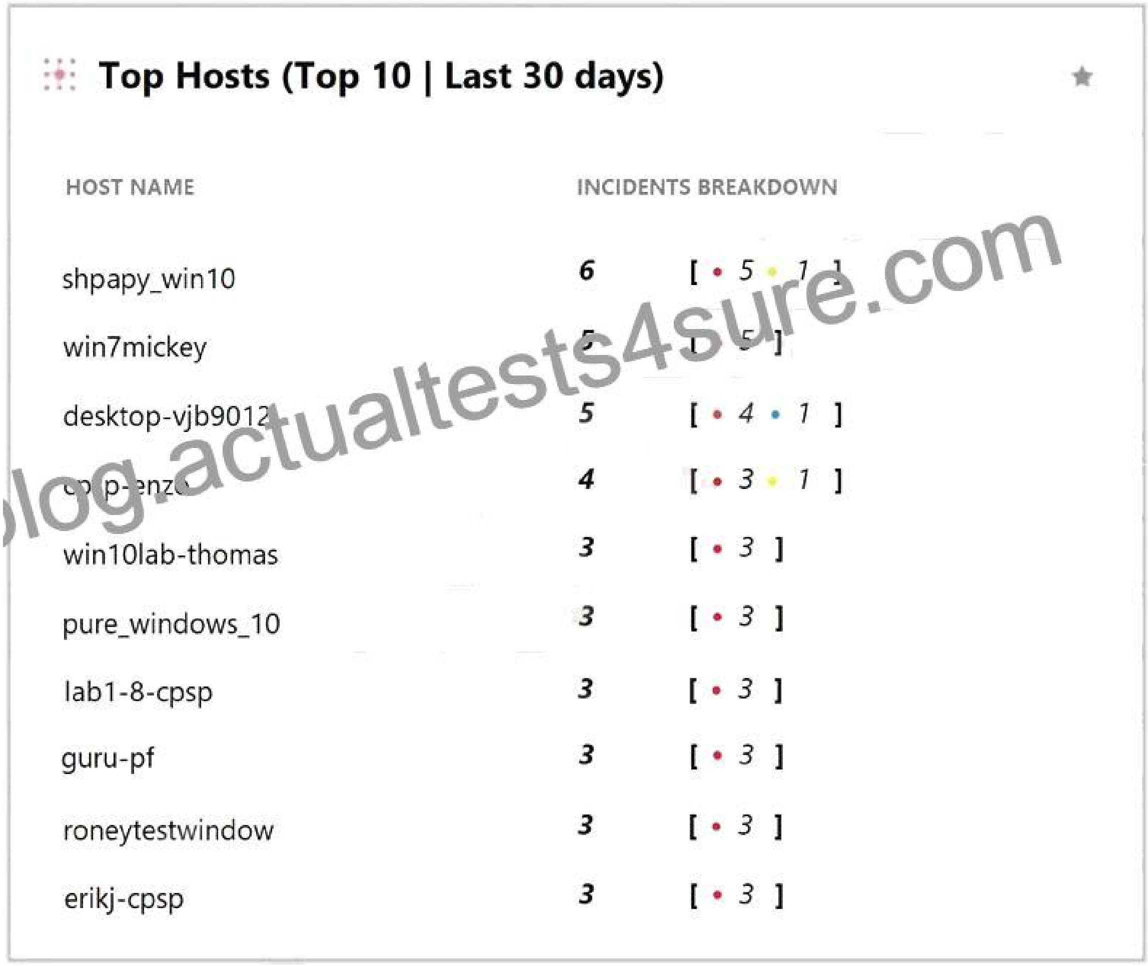

[May-2022 Newly Released] Pass PCDRA Exam - Real Questions & Answers [Q13-Q28]

[May-2022 Newly Released] Pass PCDRA Exam - Real Questions and Answers
Pass PCDRA Review Guide, Reliable PCDRA Test Engine

Palo Alto Networks PCDRA Exam Syllabus Topics:

TopicDetailsTopic 1- Characterize the differences between application protection and kernel protection- Characterize the differences between malware and exploitsTopic 2- Identify the connection of analytic detection capabilities to MITRE- List the options to highlight or suppress incidentsTopic 3- Identify common investigation screens and processes- Describe what actions can be performed using the live terminalTopic 4- Explain the purpose and use of the query builder technique- Explain the purpose and use of the IOC techniqueTopic 5- Describe how to use the Broker as a proxy between the agents and XDR in the Cloud- Describe details of the ingestion methodsTopic 6- Characterize the differences between incidents and alerts- Identify the investigation capabilities of Cortex XDRTopic 7- Identify the use of malware prevention modules (MPMs)- Identify the profiles that must be configured for malware preventionTopic 8- Identify legitimate threats (true positives) vs. illegitimate threats (false positives)- Outline incident collaboration and management using XDRTopic 9- Outline how Cortex XDR ingests other non-Palo Alto Networks data sources- Describe how to use the Broker to activate PathfinderTopic 10- Define communication options- channels to and from the client- Distinguish between different proxies
Topic 11- Distinguish between automatic vs. manual remediations- Describe how to fix false positives- Describe basic remediation
Topic 12- Define product modules that help identify threats- Summarize the generally available references for vulnerabilitiesTopic 13 - Outline distributing and scheduling capabilities of Cortex XDR- Identify the information needed for a given audienceTopic 14 - Differentiate between exploits and malware- Outline ransomware threats- Recognize the different types of attacks

NO.13 What does the following output tell us?



Top Hosts (Top 10 | Last 30 days)

HOST NAME	INCIDENTS BREAKDOWN	
shpapy_win10	6	[● 5 ● 1]
win7mickey	5	[● 5]
desktop-vjb9012	5	[● 4 ● 1]
[illegible]p-enzo	4	[● 3 ● 1]
win10lab-thomas	3	[● 3]
pure_windows_10	3	[● 3]
lab1-8-cpsp	3	[● 3]
guru-pf	3	[● 3]
roneytestwindow	3	[● 3]
erikj-cpsp	3	[● 3]

* There is one low severity incident.
* Host shpapy_win10 had the most vulnerabilities.
* There is one informational severity alert.
* This is an actual output of the Top 10 hosts with the most malware.

NO.14 Where would you view the WildFire report in an incident?
* next to relevant Key Artifacts in the incidents details page
* under Response &#8211;> Action Center
* under the gear icon &#8211;> Agent Audit Logs
* on the HUB page at apps.paloaltonetworks.com

NO.15 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.16 Live Terminal uses which type of protocol to communicate with the agent on the endpoint?
* NetBIOS over TCP

* WebSocket
* UDP and a random port
* TCP, over port 80

NO.17 After scan, how does file quarantine function work on an endpoint?
* Quarantine takes ownership of the files and folders and prevents execution through access control.
* Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.
* Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.
* Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.

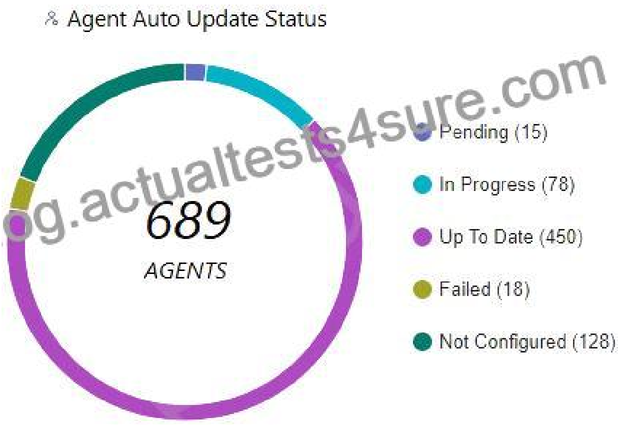
NO.18 What is by far the most common tactic used by ransomware to shut down a victim&#8217;s operation?
* preventing the victim from being able to access APIs to cripple infrastructure
* denying traffic out of the victims network until payment is received
* restricting access to administrative accounts to the victim
* encrypting certain files to prevent access by the victim

NO.19 Which of the following policy exceptions applies to the following description?

&#8216;An exception allowing specific PHP files&#8217;
* Support exception
* Local file threat examination exception
* Behavioral threat protection rule exception
* Process exception

NO.20 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.21 Which statement is true based on the following Agent Auto Upgrade widget?



* There are a total of 689 Up To Date agents.
* Agent Auto Upgrade was enabled but not on all endpoints.

* Agent Auto Upgrade has not been enabled.
* There are more agents in Pending status than In Progress status.

NO.22 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.23 You can star security events in which two ways? (Choose two.)
* Create an alert-starring configuration.
* Create an Incident-starring configuration.
* Manually star an alert.
* Manually star an Incident.

NO.24 What kind of the threat typically encrypts user files?
* ransomware
* SQL injection attacks
* Zero-day exploits
* supply-chain attacks

NO.25 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 ~= &#8220;.*?.(?:pdf|docx).exe&#8221;
* dataset = xdr_data

| filter event_type = PROCESS and

event_sub_type = PROCESS_START and

action_process_image_name ~= &#8220;.*?.(?:pdf|docx).exe&#8221;
* dataset = xdr_data

| filter action_process_image_name ~= &#8220;.*?.(?:pdf|docx).exe&#8221;

| fields action_process_image
* dataset = xdr_data

| filter event_behavior = true

event_sub_type = PROCESS_START and

action_process_image_name ~= &#8220;.*?.(?:pdf|docx).exe&#8221;

NO.26 When using the &#8220;File Search and Destroy&#8221; feature, which of the following search hash type is supported?
* SHA256 hash of the file
* AES256 hash of the file

* MD5 hash of the file
* SHA1 hash of the file

NO.27 Which profiles can the user use to configure malware protection in the Cortex XDR console?
* Malware Protection profile
* Malware profile
* Malware Detection profile
* Anti-Malware profile

NO.28 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 &#8211; False Positive

100% Free PCDRA Daily Practice Exam With 62 Questions: https://www.actualtests4sure.com/PCDRA-test-questions.html]