

PCDRA^{Q&As}

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Free Download Real Questions & Answers PDF and VCE file from:

https://www.pass4itsure.com/pcdra.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers



VCE & PDF Pass4itSure.com

https://www.pass4itsure.com/pcdra.html

2024 Latest pass4itsure PCDRA PDF and VCE dumps Download

QUESTION 1

Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

- A. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.
- B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.
- C. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.
- D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the

list, and apply it.

Correct Answer: B

QUESTION 2

What kind of the threat typically encrypts user files?

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

Correct Answer: A

QUESTION 3

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATTandCKTM techniques.

- A. Exfiltration, Command and Control, Collection
- B. Exfiltration, Command and Control, Privilege Escalation
- C. Exfiltration, Command and Control, Impact
- D. Exfiltration, Command and Control, Lateral Movement

Correct Answer: D

QUESTION 4

https://www.pass4itsure.com/pcdra.html 2024 Latest pass4itsure PCDRA PDF and VCE dumps Download

With a Cortex XDR Prevent license, which objects are considered to be sensors?

- A. Syslog servers
- B. Third-Party security devices
- C. Cortex XDR agents
- D. Palo Alto Networks Next-Generation Firewalls

Correct Answer: C

QUESTION 5

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]	
cpsp-enzo	4	[• 3 • 1]	
win 10 lab-thomas	3	[•3]	
pure_windows_10	3	[•3]	
lab1-8-cpsp	3	[•3]	
guru-pf	3	[•3]	
roneytestwindow	3	[•3]	
erikj-cpsp	3	[•3]	

A. There is one low severity incident.



https://www.pass4itsure.com/pcdra.html

2024 Latest pass4itsure PCDRA PDF and VCE dumps Download

- B. Host shpapy_win10 had the most vulnerabilities.
- C. There is one informational severity alert.
- D. This is an actual output of the Top 10 hosts with the most malware.

Correct Answer: D

Latest PCDRA Dumps

PCDRA VCE Dumps

PCDRA Study Guide