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

QUESTION 1

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C

Explanation: Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities12. Let\\'s briefly discuss the other options to provide a comprehensive explanation:

A. Unit 42 is not responsible for automation and orchestration of products. Automation and orchestration are capabilities that are provided by Palo Alto Networks products such as Cortex XSOAR, which is a security orchestration, automation and response platform that helps security teams automate tasks, coordinate actions and manage incidents3. B. Unit 42 is not responsible for the configuration optimization of the Cortex XDR server. The Cortex XDR server is the cloud-based platform that provides detection and response capabilities across network, endpoint and cloud data sources. The configuration optimization of the Cortex XDR server is the responsibility of the Cortex XDR administrators, who can use the Cortex XDR app to manage the settings and policies of the Cortex XDR server4.

C. Unit 42 is not responsible for the rapid deployment of Cortex XDR agents. The Cortex XDR agents are the software components that are installed on endpoints to provide protection and visibility. The rapid deployment of Cortex XDR agents is the responsibility of the Cortex XDR administrators, who can use various methods such as group policy objects, scripts, or third-party tools to deploy the Cortex XDR agents to multiple endpoints5. In conclusion, Unit 42 is the threat intelligence and response team of Palo Alto Networks that is responsible for threat research, malware analysis and threat hunting. By leveraging the expertise and insights of Unit 42, organizations can enhance their security posture and protect against the latest cyberthreats. References: About Unit 42: Our Mission and Team Unit 42: Threat Intelligence and Response Cortex XSOAR Cortex XDR Pro Admin Guide: Manage Cortex XDR Settings and Policies Cortex XDR Pro Admin Guide: Deploy Cortex XDR Agents

QUESTION 2

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

A. Remediation Automation

B. Machine Remediation

C. Automatic Remediation

D. Remediation Suggestions

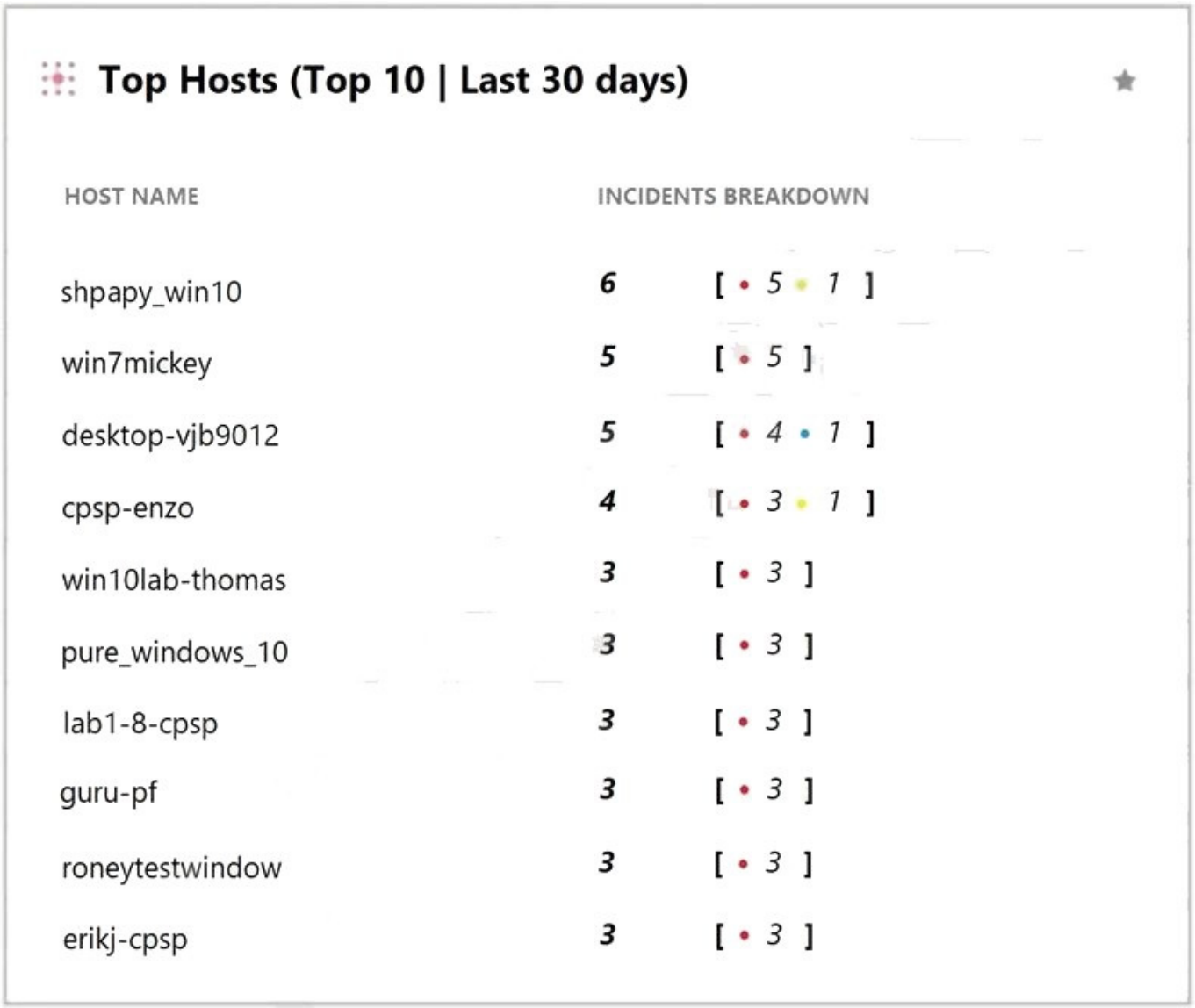
Correct Answer: D

Explanation: When investigating security events, the feature in Cortex XDR that is useful for reverting the changes on

the endpoint is Remediation Suggestions. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR. References: Remediation Suggestions Apply Remediation Suggestions

QUESTION 3

What does the following output tell us?



A. There is one low severity incident.

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

Explanation: The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more . References: Use the ACC to Analyze Network Activity Top 10 Hosts with the Most Malware

QUESTION 4

Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

A. exception profiles that apply to specific endpoints

B. agent exception profiles that apply to specific endpoints

C. global exception profiles that apply to all endpoints

D. role-based profiles that apply to specific endpoints

Correct Answer: BC

Explanation: Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives. References: Exception Security Profiles Create an Agent Exception Profile Create a Global Exception Profile

QUESTION 5

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

A. Manually remediate the problem on the endpoint in question.

B. Open X2go from the Cortex XDR console and delete the file via X2go.

C. Initiate Remediate Suggestions to automatically delete the file.

D. Open an NFS connection from the Cortex XDR console and delete the file.

Correct Answer: C

Explanation: The best action to delete the file on the Linux endpoint is to initiate Remediation Suggestions from the Cortex XDR console. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to

undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or

incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore

the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR.

The other options are incorrect for the following reasons:

A is incorrect because manually remediating the problem on the endpoint is not a convenient or efficient way to delete the file. Manually remediating the problem would require you to access the endpoint directly, log in as root, locate the file,

and delete it. This would also require you to have the necessary permissions and credentials to access the endpoint, and to know the exact path and name of the file. Manually remediating the problem would also not provide you with any

audit trail or confirmation of the deletion.

B is incorrect because opening X2go from the Cortex XDR console is not a supported or secure way to delete the file. X2go is a third-party remote desktop software that allows you to access Linux endpoints from a graphical user interface.

However, X2go is not integrated with Cortex XDR, and using it would require you to install and configure it on both the Cortex XDR console and the endpoint. Using X2go would also expose the endpoint to potential network attacks or

unauthorized access, and would not provide you with any audit trail or confirmation of the deletion.

D is incorrect because opening an NFS connection from the Cortex XDR console is not a feasible or reliable way to delete the file. NFS is a network file system protocol that allows you to access files on remote servers as if they were local.

However, NFS is not integrated with Cortex XDR, and using it would require you to set up and maintain an NFS server and client on both the Cortex XDR console and the endpoint. Using NFS would also depend on the network availability

and performance, and would not provide you with any audit trail or confirmation of the deletion.

References:

Remediation Suggestions

Apply Remediation Suggestions