PCDRA$^{\text{Q\&As}}$

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.geekcert.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

Live Terminal 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

Correct Answer: B

Explanation: Live Terminal uses the WebSocket protocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic. References: Initiate a Live Terminal Session WebSocket

QUESTION 2

What types of actions you can execute with live terminal session?

A. Manage Network configurations, Quarantine Files, Run PowerShell scripts

B. Manage Processes, Manage Files, Run Operating System Commands, Run Ruby Commands and Scripts

C. Apply patches, Reboot System, send notification for end user, Run Python Commands and Scripts

D. Manage Processes, Manage Files, Run Operating System Commands, Run Python Commands and Scripts

Correct Answer: D

Explanation: Live terminal session is a feature of Cortex XDR that allows you to remotely access and control endpoints from the Cortex XDR console. With live terminal session, you can execute various actions on the endpoints, such as: Manage Processes: You can view, start, or kill processes on the endpoint, and monitor their CPU and memory usage. Manage Files: You can view, create, delete, or move files and folders on the endpoint, and upload or download files to or from the endpoint. Run Operating System Commands: You can run commands on the endpoint using the native command-line interface of the operating system, such as cmd.exe for Windows, bash for Linux, or zsh for macOS. Run Python Commands and Scripts: You can run Python commands and scripts on the endpoint using the Python interpreter embedded in the Cortex XDR agent. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint. References: Initiate a Live Terminal Session Manage Processes Manage Files Run Operating System Commands Run Python Commands and Scripts

QUESTION 3

When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

A. The agent technical support file.

B. The prevention archive from the alert.

C. The distribution id of the agent.

D. A list of all the current exceptions applied to the agent.

E. The unique agent id.

Correct Answer: AB

Explanation: When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are: The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself. The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself. The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example: The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder. A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent\\'s security policies. The exceptions can help TAC understand the agent\\'s configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file. The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file. References: Generate and Download the Agent Technical Support File Generate and Download the Prevention Archive Cortex XDR Agent Administrator Guide: Agent Distribution ID Cortex XDR Agent Administrator Guide: Exception Security Profiles [Cortex XDR Agent Administrator Guide: Unique Agent ID]

QUESTION 4

Which version of python is used in live terminal?

A. Python 2 and 3 with standard Python libraries

B. Python 2 and 3 with specific XDR Python libraries developed by Palo Alto Networks

C. Python 3 with specific XDR Python libraries developed by Palo Alto Networks

D. Python 3 with standard Python libraries

Correct Answer: D

Explanation: Live terminal uses Python 3 with standard Python libraries to run Python commands and scripts on the endpoint. Live terminal does not support Python 2 or any custom or external Python libraries. Live terminal uses the Python interpreter embedded in the Cortex XDR agent, which is based on Python 3.7.4. The standard Python libraries are the modules that are included with the Python installation and provide a wide range of functionalities, such as operating system interfaces, network programming, data processing, and more. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint, such as querying system information, modifying files or registry keys, or running other applications. References: Run Python Commands and Scripts Python Standard Library

QUESTION 5

What is the action taken out by Managed Threat Hunting team for Zero Day Exploits?

A. MTH researches for threats in the tenant and generates a report with the findings.

B. MTH researches for threats in the logs and reports to engineering.

C. MTH runs queries and investigative actions and no further action is taken.

D. MTH pushes content updates to prevent against thezero-dayexploits.

Correct Answer: A

Explanation: The Managed Threat Hunting (MTH) team is a group of security experts who proactively hunt for threats in the Cortex XDR tenant and generate a report with the findings. The MTH team uses advanced queries and investigative actions to identify and analyze potential threats, such as zero-day exploits, that may have bypassed the prevention and detection capabilities of Cortex XDR. The MTH team also provides recommendations and best practices to help customers remediate the threats and improve their security posture. References: Managed Threat Hunting Service Managed Threat Hunting Report