Exam : **PSE-Cortex-Pro-24**

Title : Palo Alto Networks Systems Engineer Professional - Cortex

Vendor : Palo Alto Networks

Version : DEMO

NO.1 An adversary attempts to communicate with malware running on a network in order to control malware activities or to exfiltrate data from the network.
Which Cortex XDR Analytics alert will this activity most likely trigger?
A. uncommon local scheduled task creation
B. malware
C. new administrative behavior
D. DNS Tunneling
Answer: D
Reference: https://www.boll.ch/datasheets/Cortex_XDR_for_Network_Traffic_Analysis.pdf

NO.2 Which integration allows searching and displaying Splunk results within Cortex XSOAR?
A. SplunkPY integration
B. Demisto App for Splunk integration
C. XSOAR REST API integration
D. Splunk integration
Answer: A
Reference: https://xsoar.pan.dev/docs/reference/integrations/splunk-py

NO.3 Which integration allows data to be pushed from Cortex XSOAR into Splunk?
A. ArcSight ESM integration
B. SplunkUpdate integration
C. Demisto App for Splunk integration
D. SplunkPY integration
Answer: D
Reference: https://xsoar.pan.dev/docs/reference/integrations/splunk-py

NO.4 A Cortex XSOAR customer wants to ingest emails from a single mailbox. The mailbox brings in reported phishing emails and email requests from human resources (HR) to onboard new users. The customer wants to run two separate workflows from this mailbox, one for phishing and one for onboarding.
What will allow Cortex XSOAR to accomplish this in the most efficient way?
A. Create two instances of the email integration and classify one instance as ingesting incidents of type phishing and the other as ingesting incidents of type onboarding.
B. Use an incident classifier based on a field in each type of email to classify those containing "Phish Alert" in the subject as phishing and those containing "Onboard Request" as onboarding.
C. Create a playbook to process and determine incident type based on content of the email.
D. Use machine learning (ML) to determine incident type.
Answer: B
Reference: https://xsoar.pan.dev/docs/reference/packs/email-communication

NO.5 Which two entities can be created as a BIOC? (Choose two.)
A. file
B. registry

C. event log
D. alert log
Answer: A B
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex- xdr-indicators/working-with-biocs/create-a-bioc-rule.html

NO.6 What does Cortex Xpanse ingest from XDR endpoints?
A. MAC addresses
B. User-agent data
C. Public IP addresses
D. Hostnames
Answer: C
Explanation:
Cortex Xpanse ingests public IP addresses from XDR endpoints. This allows the platform to monitor and track internet-facing assets, providing visibility into exposed assets and potential attack surfaces across the network.

NO.7 Which command-line interface (CLI) query would retrieve the last three Splunk events?
A. !search using=splunk_instance_1 query="* | last 3"
B. !search using=splunk_instance_1 query="* | 3"
C. !query using=splunk_instance_1 query="* | last 3"
D. !search using=splunk_instance_1 query="* | head 3"
Answer: D

NO.8 What is the primary function of an engine in Cortex XSOAR?
A. To execute playbooks, scripts, commands, and integrations
B. To manage multiple Cortex XSOAR tenants
C. To provide a user interface for security analysts
D. To store and manage incident data, remediation plans, and documentation
Answer: A
Explanation:
The primary function of an engine in Cortex XSOAR is to execute playbooks, scripts, commands, and integrations. This allows the platform to automate and orchestrate security operations tasks, helping security teams respond to incidents more efficiently.

NO.9 What are the key capabilities of the ASM for Remote Workers module?
A. Monitoring endpoint activity, managing firewall rules, and mitigating cybersecurity threats
B. Gathering endpoint data, conducting internal scans, and automating network configurations
C. Identifying office network vulnerabilities, monitoring remote workforce, and encrypting data
D. Analyzing global scan data, identifying risky issues on remote networks, and providing internal insights
Answer: D
Explanation:

The ASM for Remote Workers module in Cortex Xpanse focuses on analyzing global scan data, identifying risky issues on remote networks, and providing internal insights. This helps organizations maintain visibility and control over the security of their remote workforce, ensuring that potential risks and vulnerabilities in remote network configurations are addressed proactively.

NO.10 What is the primary mechanism for the attribution of attack surface data in Cortex Xpanse?

A. Active scanning with network-installed agents

B. Dark web monitoring

C. Customer-provided asset inventory lists

D. Scanning from public internet data sources

Answer: D

Explanation:

The primary mechanism for the attribution of attack surface data in Cortex Xpanse is scanning from public internet data sources. Cortex Xpanse continuously scans the internet to identify assets that are potentially exposed or vulnerable, providing a comprehensive view of an organization's attack surface based on public- facing data.

NO.11 Which solution profiles network behavior metadata, not payloads and files, allowing effective operation regardless of encrypted or unencrypted communication protocols, like HTTPS?

A. endpoint protection platform (EPP)

B. Security Information and Event Management (SIEM)

C. endpoint detection and response (EDR)

D. Network Detection and Response (NDR)

Answer: D

Reference: https://www.paloaltonetworks.com/cyberpedia/what-is-network-detection-and-response

NO.12 How does a clear understanding of a customer's technical expertise assist in a hand off following the close of an opportunity?

A. It enables customers to prepare for audits so they can demonstrate compliance.

B. It helps in assigning additional technical tasks to the customer

C. It allows implementation teams to bypass initial scoping exercises

D. It enables post-sales teams to tailor their support and training appropriately

Answer: D

Explanation:

A clear understanding of a customer's technical expertise helps post-sales teams customize their support and training efforts to match the customer's knowledge level. This ensures that the customer receives the appropriate guidance, training, and resources needed to effectively use the product or solution after the sale.

NO.13 Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR? (Choose two)

A. Security Event

B. HIP

C. Correlation
D. Analytics
Answer: A B

NO.14 Which two types of indicators of compromise (IOCs) are available for creation in Cortex XDR? (Choose two.)
A. registry
B. file path
C. hash
D. hostname
Answer: B C

NO.15 Which feature of Cortex XSIAM displays an entire picture of an attack, including the originating process or delivery point?
A. Sample analysis
B. Correlation rule
C. Causality View
D. Automation playbook
Answer: C
Explanation:
The Causality View in Cortex XSIAM provides an entire picture of an attack, including the originating process or delivery point. It allows security teams to visualize and understand the full sequence of events leading to an attack, helping to identify root causes and mitigate future risks.

NO.16 What allows the use of predetermined Palo Alto Networks roles to assign access rights to Cortex XDR users?
A. role-based access control
B. cloud identity engine
C. endpoint groups
D. restrictions security profile
Answer: A
Reference: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide
/Manage-User-Roles

NO.17 What does DBot use to score an indicator that has multiple reputation scores?
A. most severe score
B. undefined score
C. average score
D. least severe score
Answer: A
Reference: https://xsoar.pan.dev/docs/integrations/dbot