Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
In the MITRE ATT&CK framework, which term describes the specific high-level "Why" or goal of an attacker, such as "Initial Access" or "Exfiltration"?

A. Technique
B. Tactic
C. Procedure
D. Mitigation

Answer: B

Explanation:
TheMITRE ATT&CKframework is categorized into a hierarchy that helps SOC analysts understand attacker behavior:
Tactic (B):This is theobjective/goalof the attacker. There are currently 14 tactics in the Enterprise matrix, including Reconnaissance, Persistence, and Lateral Movement. It answers the question "What is the attacker trying to achieve?"
Technique (A):This is the "How"—the specific method used to achieve a tactic (e.g., "Spearphishing Attachment" to achieve "Initial Access").
Procedure (C):The specific implementation or "recipe" used by a particular threat actor (e.g., "APT28 used a specific PowerShell script to bypass AMSI").
Mapping:Cortex XDR and XSIAM natively map alerts to these Tactics and Techniques to help analysts quickly understand the stage and intent of an attack.

NEW QUESTION 2
Which two types of tasks are supported in Cortex XSIAM playbooks? (Choose two.)

A. Sub-playbook
B. Script creation
C. Conditional
D. Data collection

Answer: AC

NEW QUESTION 3
A customer is investigating a security incident in which unusual network traffic is observed and a malicious process is identified on an endpoint. Which Cortex XDR capability assists with correlating firewall network logs and endpoint data in this environment?

A. Log stitching
B. User authentication management
C. Indicator of compromise (IOC) rule
D. Analytics

Answer: A

Explanation:
In the Palo Alto Networks Cortex XDR ecosystem,Log Stitchingis the fundamental technology that enables the "X" (Extended) in XDR. It is the process of automatically reassembling fragmented data from disparate sources—such as Next-Generation Firewalls (NGFW), GlobalProtect, and the Cortex XDR agent—into a single, cohesive narrative.
How it Works:When a firewall identifies a network flow and an endpoint agent identifies a process execution, these are initially two separate logs. Cortex XDR uses "stitching" to link these logs by matching common attributes (such as timestamps, source/destination IP addresses, and ports) to identify theCausality Group Owner (CGO).
The Result:This allows an analyst to see exactly which local process on the endpoint (e.g., powershell.exe) was responsible for generating the specific malicious network traffic caught by the firewall. Without log stitching, these would remain two isolated events, making it much harder to prove the "cause and effect" of an attack.
Why other options are incorrect:
User authentication management:Focuses on identity and access, not the correlation of network and process telemetry.
Indicator of compromise (IOC) rule:These are typically used to flag known malicious artifacts (like a specific file hash or IP address) but do not perform the structural correlation of different log types.
Analytics:While Analyticsusesthe data provided by log stitching to identify behavioral anomalies, the specific capability that performs the correlation and "linking" of the firewall and endpoint logs is the stitching process itself.

NEW QUESTION 4
What is the Cortex XSOAR Marketplace?

A. Searchable collection of third-party playbooks and data models
B. Development environment for creating and sharing third-party integrations
C. Digital storefront where Cortex XSOAR training credits can be purchased and used
D. Built-in repository of installable content, including integrations and automations

Answer: D

NEW QUESTION 5
How does the "Unit 42 Intel" integration directly assist a SOC analyst within the Cortex XDR or XSIAM Incident view?

A. It automatically resets the user's password in Active Directory.
B. It provides a "threat card" with actor profiles, known aliases, and related MITRE ATT&CK techniques.
C. It opens a 24/7 chat window with a dedicated Unit 42 forensic investigator.
D. It provides the source code of the malware identified in the incident.

Answer: B

NEW QUESTION 6
Which process in Cortex XSIAM ensures that raw logs from different vendors (e.g., Check Point, Cisco, and Microsoft) are converted into a standardized format for unified analysis?

A. Data Stitching
B. XDM Mapping
C. Entity Profiling
D. Log Ingestion

Answer: B

Explanation:
TheXDM (Cortex Data Model)is the backbone of Cortex XSIAM's ability to act as a unified SOC platform.
Standardization:Raw logs come in many formats (Syslog, JSON, LEEF).XDM Mappingis the process of taking those raw fields and "mapping" them to a common schema. For example, "src_ip," "source_address," and "sIP" from different vendors are all mapped to a single XDM field called xdm.source.ipv4.
Cross-Vendor Correlation:Once data is mapped to XDM, an analyst can write one XQL query that searches across logs fromallvendors simultaneously, which is essential for effective threat hunting in a multi-vendor environment.

NEW QUESTION 7
Which metric is used by SOC management to measure the average "Dwell Time"—the duration between a successful compromise and the moment it is first identified by a security tool or analyst?

A. MTTR (Mean Time to Respond)
B. MTTA (Mean Time to Acknowledge)
C. MTTD (Mean Time to Detect)
D. MTTC (Mean Time to Contain)

Answer: C

NEW QUESTION 8
Which Cortex XSOAR feature is used to ensure that specific data points from an incoming alert (such as a "Source_Address" from a firewall log) are correctly assigned to the standardized "Source IP" field within the XSOAR incident?

A. Classification
B. Mapping
C. Data Normalization
D. Playbook Transformation

Answer: B

Explanation:
In Cortex XSOAR, the process of handling incoming data involves two distinct steps:ClassificationandMapping.
Classification:Determineswhatthe incident is (e.g., "This is a Phishing incident").
Mapping (B):Once the incident type is known, Mapping is used to "link" the raw data from the source integration to the fields in the XSOAR incident. For example, if a third-party tool sends an IP in a field called src, theMapperensures that value is placed into the XSOAR incident field sourceip.
Consistency:This ensures that regardless of which tool detected the threat, the analyst and the playbooks always see the data in the same standardized fields, which is essential for automation to work correctly.

NEW QUESTION 9
What is the role of content packs in Cortex XSOAR?

A. To provide pre-built bundles for supporting security orchestration use cases
B. To support technical support teams with relevant information required to troubleshoot
C. To serve as a central location for installing, exchanging, and contributing content
D. To serve as a major software versioning update

Answer: A

Explanation:
In Cortex XSOAR,Content Packsare the essential building blocks used to implement security orchestration, automation, and response (SOAR) workflows.
Pre-built Bundles:A content pack is a comprehensive, version-controlled bundle that includes all the components necessary for a specific security use case. This typically includes integrations (to connect to 3rd party tools), playbooks (the logic of the workflow), automation scripts, layouts, fields, and dashboards.
Rapid Deployment:Instead of building a phishing response workflow from scratch, an administrator can install the "Phishing" content pack from the Marketplace. This immediately provides the out-of-the-box (OOTB) logic required to handle that specific threat.
Note on Option C:While Option C describes theCortex XSOAR Marketplaceitself, therole of the content packis the actual delivery of the pre-built logic and tools defined in Option A.

NEW QUESTION 10
Where is the data retrieved by an integration task (such as a user's email address or a file's reputation) stored within an incident so that other playbook tasks can access it?

A. War Room
B. Context Data
C. Incident Fields
D. Evidence Board

Answer: B

NEW QUESTION 10
What is a difference between cold storage and hot storage in Cortex?

A. Cold storage is required, while hot storage is optional.
B. Cold storage and hot storage can be stored in different cloud locations.
C. Logs in cold storage have more details than logs stored in hot storage.
D. Querying logs in cold storage takes more time than querying logs in hot storage.

Answer: D

NEW QUESTION 12
A new incident in Cortex XSIAM contains WildFire malware and Behavioral Threat Protection (BTP) alerts about an unsigned process attempting to dump the memory of lsass.exe. Which initial verdict applies to this incident?

A. False positive
B. True positive
C. False negative
D. True negative

Answer: B

NEW QUESTION 17
What is enabled by Role-Based Access Control (RBAC) in Cortex XDR?

A. Management of permissions and assignment of administrator access rights.
B. Ability to manage Cortex XDR features based on job function.
C. Automated response to detected threats based on user roles.
D. Granular control and visibility over network traffic policies based on user roles.

Answer: A

NEW QUESTION 19
Which task should a threat hunter include in the investigation when a Cortex XDR incident contains alerts about a malicious process?

A. Immediately isolate the endpoint and delete the identified file.
B. Search for the SHA256 file hash on other endpoints in the environment.
C. Add the SHA256 file hash to the Cortex XDR global block list.
D. Disable the account of the user responsible for initiating the process.

Answer: B

NEW QUESTION 24
Which solution will minimize mean time to resolution (MTTR) when, as a result of previous malware infection, a company??s Windows endpoint is suffering a small amount of file corruption and modified registry keys?

A. Issue a new laptop from the help desk to expedite a clean system.
B. Use Live Terminal to connect to the machine and upload files to replace the corrupted files.
C. Use group policy objects to push new files and registry key changes to the endpoint.
D. Use remediation suggestions to restore the affected files and registry modifications.

Answer: D

NEW QUESTION 25
Which scripting language would create a custom widget in Cortex XDR that shows the top five accounts with failed Windows logons in the past 24 hours?

A. XQL
B. JavaScript
C. Python
D. PowerShell

Answer: A

NEW QUESTION 30
.....

Relate Links

100% Pass Your SecOps-Pro Exam with Exambible Prep Materials

https://www.exambible.com/SecOps-Pro-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/