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
Which action should an administrator take to create automated response actions when a user account is compromised? (Choose one answer)

A. Map the events as a type of Cortex XSOAR incident, then run a playbook.
B. Run a custom script from the Cortex XDR script library.
C. Create a script in Cortex XSOAR that will run a playbook based on the scenario.
D. Create playbook triggers in Cortex XSIAM and run playbooks for each alert.

Answer: A

NEW QUESTION 2
Which Cortex XDR Exploit Prevention Module (EPM) is specifically designed to detect and block "Return-Oriented Programming" (ROP) techniques by monitoring for "stack pivoting" or "jump to return" instructions?

A. Anti-Exploit Core
B. JMP2RET / Stack Pivot Protection
C. Local Privilege Escalation Protection
D. DLL Security

Answer: B

NEW QUESTION 3
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 4
Which Cortex XSIAM component uses machine learning to automatically build a baseline of "normal" behavior for every user and host in the network, and then provides a searchable profile of their historical activity and risk level?

A. XQL Engine
B. Entity Profiling
C. Broker VM
D. Data Ingestion Service

Answer: B

Explanation:
Entity Profilingis the specific Cortex XSIAM capability that powers its User and Entity Behavioral Analytics (UEBA) functions.
Baselining:For every entity (a user account or a host/device), the system observes its standard operations—such as which servers it connects to, what time it typically logs in, and what applications it runs.
Searchable Profiles:Analysts can use theEntity Explorerto view a "Profile" for any user. This profile includes a "Risk Score" and a summary of all anomalies associated with that entity over time.
Security Context:This allows a SOC analyst to quickly answer the question: "Is this user's current behavior (e.g., accessing a sensitive database) normal forthem, or is it a sign of credential theft?"
Difference from XQL (A):XQL is the language used toquerythe data, but Entity Profiling is the background process and engine thatbuildsthe behavioral models and stores the entity-specific context.

NEW QUESTION 5
According to the Traffic Light Protocol (TLP) 2.0 standard, which classification is used for information that is restricted to the specific individuals involved in an investigation and cannot be shared further?

A. TLP:CLEAR
B. TLP:GREEN
C. TLP:AMBER
D. TLP:RED

Answer: D

NEW QUESTION 6
How do sensors function in Cortex XSIAM?

A. They monitor endpoint agent health.

B. They monitor data ingestion health.
C. They assist with log stitching.
D. They collect logs and telemetry data.

Answer: D

NEW QUESTION 7
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 8
Which two functions are allowed when stitching logs in Cortex XDR? (Choose two.)

A. Providing real-time threat prevention or remediation of threats
B. Creating granular BIOC and correlation rules
C. Enabling creation of custom scripts for remediation of security incidents
D. Running investigation queries based on combined network and endpoint events

Answer: BD

NEW QUESTION 9
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 10
Which two statements are relevant to reports in Cortex XDR? (Choose two.)

A. They can be sent in a password protected PDF version.
B. They can be automatically pushed to the corporate intranet.
C. They can use mock data for visualization.
D. They can have an attached screenshot of an XQL query widget.

Answer: AD

NEW QUESTION 10
Which component of Cortex XDR is designed to detect insider threats?

A. Forensics
B. Identity Analytics
C. Cloud Identity Engine
D. Host Insights

Answer: B

Explanation:
Identity Analytics(formerly part of the Magnifier module) is specifically designed to identify stealthy attacks that traditional signature-based tools miss, such asinsider threats, credential theft, and lateral movement.
Behavioral Baselining:It uses Machine Learning to create a "baseline" of normal behavior for every user and entity in the network. It tracks who they usually communicate with, what time they log in, and what resources they typically access.
Anomaly Detection:If a user suddenly begins accessing sensitive servers they??ve never touched before or starts transferring large amounts of data to an unusual external IP, Identity Analytics flags this as a "User Behavioral Analytics" (UBA) alert.
Focus on Identity:Unlike Host Insights (which looks at vulnerabilities) or Forensics (which looks at disk artifacts), Identity Analytics focuses purely on theactions of the user accountto find malicious intent.

NEW QUESTION 12
During a sophisticated cyber attack, a company experiences a stealthy, multivector intrusion that evades detection by traditional security tools. The company requires a solution that will correlate and analyze the disparate attack indicators across its network, endpoints, and cloud environments to uncover the full scope of the breach and take immediate automated response actions. Which solution should be recommended?

A. XDR
B. SIEM
C. EDR
D. XSOAR

Answer: A

NEW QUESTION 14
What can be used to triage and determine if an artifact in Cortex XDR is malicious?
(Choose one answer)

A. Alert severity
B. MITRE tactic
C. SmartScore
D. WildFire report

Answer: D

NEW QUESTION 19
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 24
.....

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/