



Vendor: Palo Alto Networks

Exam Code: SecOps-Pro

Exam Name: Palo Alto Security Operations Professional

Version: DEMO

QUESTION 1

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 in Cortex XDR analyzes user behavior and access patterns to detect insider threats.

QUESTION 2

A new incident in Cortex XSIAM contains WildFire malware and Behavioral Threat Protection (BTP) alerts out 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

Explanation:

Alerts from WildFire and Behavioral Threat Protection on an unsigned process dumping LSASS memory indicate malicious activity, making it a true positive.

QUESTION 3

A file hash is evaluated a Cortex XSOAR by using two unique threat feeds:

- VirusTotal feed (rating of B- usually reliable) and the file verdict is malicious
- AlienVault feed (rating of B- usually reliable) and the file verdict is benign

What is the file verdict in XSOAR?

- A. Benign
- B. Malicious
- C. Unknown
- D. Suspicious

Answer: C

Explanation:

Conflicting threat feed verdicts (malicious vs. benign) result in an "Unknown" verdict in Cortex XSOAR until further analysis resolves the conflict.

QUESTION 4

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: D

Explanation:

The Analytics component correlates endpoint data and firewall logs to detect complex attack patterns and suspicious activity.

QUESTION 5

Where can an administrator begin to grant a new non-SSO user access to a Cortex XDR tenant?

- A. Cortex XDR tenant settings under Access Management
- B. Cortex Gateway
- C. Customer Support Portal
- D. IT Service Portal

Answer: A

Explanation:

Access Management in Cortex XDR tenant settings is where administrators grant new non-SSO users access.

QUESTION 6

Where can the actions taken to stitch alerts together in Cortex XSIAM be viewed?

- A. Alerts and Insights
- B. Timeline
- C. Causality chain
- D. Key Assets & Artifacts

Answer: C

Explanation:

The causality chain in Cortex XSIAM visualizes alerts stitched together to show the sequence and relationship of events.

QUESTION 7

What determines the indicator layout displayed and the scripts that will run on an indicator of compromise (IOC) in Cortex XSIAM?

- A. Size
- B. Type
- C. Date
- D. Origin

Answer: B

Explanation:

The IOC type determines which layout and scripts are applied to an indicator of compromise in

Cortex XSIAM.

QUESTION 8

Which action is performed as the final step of the NIST incident response plan?

- A. Updating incident response procedures
- B. Gathering evidence
- C. Restoring from backups
- D. Conducting incident response training exercises

Answer: A

Explanation:

The final step in the NIST incident response plan is updating incident response procedures based on lessons learned from the incident.

QUESTION 9

What is the purpose of incident types in Cortex XSOAR?

- A. They categorize manual and automated incidents, trigger playbooks automatically, and require predefined fields and integrations.
- B. They assist in mapping manual incidents, assign default playbooks, and require inline auto-extraction of indicators.
- C. They classify events ingested through integrations or the REST API, can trigger specific playbooks, and include customizable layouts and service-level agreement (SLA) parameters.
- D. They manually create incidents, configure universal playbooks, and enforce strict adherence to preset service-level agreement (SLA) reminders.

Answer: C

Explanation:

Incident types classify events ingested via integrations or APIs, can trigger playbooks automatically, and support customizable layouts and SLA parameters.

QUESTION 10

Which activities are facilitated through the War Room in Cortex XSOAR?

- A. Creating, editing, and deleting tasks in the workplan
- B. Running security playbooks, scripts, and commands
- C. Conducting initial investigation of incident data and threat intelligence
- D. Viewing a summary of case details and alerts

Answer: B

Explanation:

The War Room in Cortex XSOAR allows analysts to run playbooks, scripts, and commands as part of investigation and response activities.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14