Boost up Your Certification Score

Paloalto Networks

PSE-Cortex-Pro-24

Palo Alto Networks Systems Engineer Professional - Cortex

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

When analyzing logs for indicators, which are used for only BIOC identification ' ?

A. observed activity
B. artifacts
C. techniques
D. error messages

Answer: C

Question: 2

What should be configured for a Cortex XSIAM customer who wants to automate the response to certain alerts?

A. Playbook triggers
B. Correlation rules
C. Incident scoring
D. Data model rules

Answer: A

Explanation:
To automate the response to certain alerts in Cortex XSIAM , playbook triggers should be configured. Playbooks allow automated workflows to be executed based on specific condit ions or alerts, enabling faster and more consistent responses to security events.

Question: 3

Which description applies to the features of the Cortex platform as a holistic ecosystem?

A. It is solely focused on reactive security measures, neglecting proactive approaches.
B. It offers an end-to-end security solution, covering every step of security processes.
C. It primarily focuses on endpoint prevention without addressing other security aspects
D. It provides a partial security solution, leaving some steps of the security process uncovered.

Answer: B

Explanation:

The Cortex platform is designed as a holistic ecosystem that offers an end-to-end security solution , covering every step of the security process. This includes prevention, detection, investigation, and response, integrating multiple technologies and services to provide comprehensive protect ion across the entire security lifecycle.

Question: 4

What is a benefit of user entity behavior analytics (UEBA) over security information and event management (SIEM)?

A. SIEMs supports only agentless scanning, not agent-based workload protection across VMs, containers/Kubernetes.
B. UEBA can add trusted signers of Windows or Mac processes to a whitelist in the Endpoint Security Manager (ESM) Console.
C. SIEMs have difficulty detecting unknown or advanced security threats that do not involve malware, such as credential theft.
D. UEBA establishes a secure connection in which endpoints can be routed, and it collects and forwards logs and files for analysis.

Answer: C

Question: 5

What method does the Traps agent use to identify malware during a scheduled scan?

A. Heuristic analysis
B. Local analysis
C. Signature comparison
D. WildFire hash comparison and dynamic analysis

Answer: D

Question: 6

Which action should be performed by every Cortex Xpanse proof of value (POV)?

A. Grant the customer access to the management console immediately following activation.
B. Provide the customer with an export of all findings at the conclusion of the POV.
C. Enable all of the attach surface rules to show the highest number of alerts.
D. Review the mapping in advance to identity a few interesting findings to share with the customer.

Answer: D

Explanation:
During a Cortex Xpanse proof of value (POV) , it ' s important to review the mapp ing in advance to identify a few interesting findings to share with the customer. This helps highlight the product ' s value and allows the customer to see actionable insights early in the evaluation process, making the POV more impactful.

Question: 7

Which aspect of Cortex Xpanse allows for visibility over remote workforce risks?

A. The ability to identify customer assets on residential networks
B. The use of a VPN connection to scan remote devices
C. The deployment of a Cortex Xpanse aqent on the remote endpoint
D. The presence of a portal for remote workers to use for posture checking

Answer: A

Explanation:
Cortex Xpanse provides visibility over remote workforce risks by identifying customer assets on residential networks. This allows organizations to monitor and secure assets that are outside of the traditional corporate network, which is particularly important as more employees work remotely and connect from various locations.

Question: 8

Where is the best place to find official resource material?

A. Online forums
B. Video series
C. Administrator ' s guide
D. Technical blogs

Answer: B

Question: 9

Where is the output of the task visible when a playbook task errors out?

A. playbook editor
B. XSOAR audit log
C. /var/log/messages
D. War Room of the incident

Answer: D

Question: 10

How can you view all the relevant incidents for an indicator?

A. Linked Incidents column in Indicator Screen
B. Linked Indicators column in Incident Screen
C. Related Indicators column in Incident Screen
D. Related Incidents column in Indicator Screen

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer