
**Vendor:** Palo Alto Networks

**Exam Code:** CloudSec-Pro

**Exam Name:** Palo Alto Networks Cloud Security Professional

**Version:** DEMO

**QUESTION 1**
Which two actions should be implemented by a SOC manager to improve the efficiency of the team's incident response process? (Choose two.)

A. Reduce the number of analysts on shift to minimize resource usage.
B. Establish a clear incident response playbook for common security incidents.
C. Implement regular training and simulation exercises.
D. Upgrade the physical security of the facility.

**Answer:** BC
**Explanation:**
Clear incident response playbooks standardize handling procedures for common threats, improving response speed and consistency. Regular training and simulation exercises strengthen analyst readiness and ensure the team can effectively respond to real-world incidents.

**QUESTION 2**
A company's SOC team and network security team operate independently but have a directive from the CISO to work more closely together due to issues resulting from a lack of cross-team collaboration. This often delays incident response, as analysts on both teams find themselves unknowingly working on the same alerts. Which solution will improve security metrics and outcomes while aligning to the directive from the CISO?

A. Implement network segmentation techniques combined with log analysis and periodic manual threat hunting
B. Integrate automated threat intelligence
C. Integrate and consolidate visibility and response capabilities across the company attack surface
D. Implement a Unified Threat Management (UTM) system

**Answer:** C
**Explanation:**
Integrating and consolidating visibility and response capabilities across the attack surface enables both SOC and network security teams to work from a unified set of alerts, telemetry, and workflows. This reduces duplicated effort, improves collaboration, and accelerates incident response outcomes.

**QUESTION 3**
In which two use cases is the use of SIEM more appropriate than the use of SOAR to investigate a user who logs in with a malicious IP address? (Choose two.)

A. Using predefined rules and patterns to identify data points
B. Enriching data and triaging alert information
C. Continuously monitoring data for pattern recognition
D. Mapping external threats to SOC incidents

**Answer:** AC
**Explanation:**
SIEM is designed for centralized log analysis, correlation, and continuous monitoring of events. It uses predefined rules and behavioral patterns to identify suspicious activity and continuously monitors data streams for threat detection and pattern recognition involving malicious IP addresses.

**QUESTION 4**
Which concept proactively enhances internal processes for incident response and management against known threats?

A. Threat intelligence
B. Security Information and Event Management (SIEM)
C. User and Entity Behavior Analytics (UEBA)
D. Endpoint detection and response (EDR)

**Answer:** A
**Explanation:**
Threat intelligence proactively improves incident response and security operations by providing actionable information about known threats, attacker tactics, and indicators of compromise that organizations can use to strengthen detection and response processes.

**QUESTION 5**
Which action should be taken to investigate multiple log sources when researching a known threat by using threat intelligence?

A. Build an XQL query using the Query Builder.
B. O Identify characteristics used to create a behavioral indicator of compromise (BIOC) or correlation rule.
C. Select an event of interest and open the Causality View.
D. Review the sequence of events in the timeline.

**Answer:** A
**Explanation:**
Building an XQL query using the Query Builder enables analysts to investigate and correlate data across multiple log sources when researching a known threat with threat intelligence, providing centralized visibility and flexible analysis capabilities.

**QUESTION 6**
How can a company use Cortex XSIAM to automate security operations and enhance threat detection?

A. Automatically implement firewall rules based on detected vulnerabilities.
B. Decrease the number of analysts needed to review an organization security posture.
C. Configure playbooks to automate response actions for detected threats.
D. Review all security logs on a daily basis and automatically create cases.

**Answer:** C
**Explanation:**
Cortex XSIAM enhances threat detection and automates security operations by using playbooks that automatically execute predefined response actions when threats are detected. This reduces manual intervention, accelerates incident response, and improves operational efficiency across the SOC.

**QUESTION 7**
Which step is required to create a user role?

A. Enter a description for the group.

B. Modify the role name.
C. Navigate to access management.
D. Create a data set.

**Answer:** C
**Explanation:**
User roles are created and managed through the Access Management section, where administrators define permissions and assign access controls for users and groups within Cortex Cloud.

**QUESTION 8**
A security engineer needs to transfer dashboard configurations between the company's Cortex Cloud environments for Asia, Europe, and North America divisions to streamline onboarding. Which condition would prevent this action?

A. Dashboards are based on custom infrastructure.
B. Dashboards are in JSON format.
C. Predefined dashboards cannot be exported.
D. Dashboards include XQL widgets.

**Answer:** C
**Explanation:**
Predefined dashboards are built into Cortex Cloud and cannot be exported or transferred between environments. Only user-created custom dashboards support export and import operations for reuse across regions or tenants.

**QUESTION 9**
When is it advantageous to deploy a Cortex XDR agent with advanced endpoint protection for a Windows host to detect a malicious occurrence?

A. When analyzing memory usage on the host
B. When simultaneously collecting information on hosts
C. When proactively collecting forensic data to analyze an event
D. When gathering a holistic view of running processes

**Answer:** C
**Explanation:**
Advanced endpoint protection in the Cortex XDR agent is advantageous because it can proactively collect forensic data related to suspicious activity, enabling detailed investigation and analysis of malicious events on Windows hosts.

**QUESTION 10**
How can an administrator use Endpoint Administrative Cleanup to ensure that all duplicates have been removed from the All Endpoints table in Cortex Cloud and that the table includes the most accurate list of endpoints?

A. Reinstall the agents on all endpoints.
B. Enable periodic duplicate cleanup and define criteria.
C. Define criteria and remove any duplicate endpoint agents.
D. Copy and then delete all duplicate entries from the table.

**Answer:** C
**Explanation:**
Endpoint Administrative Cleanup allows administrators to define cleanup criteria and remove duplicate endpoint agents so the All Endpoints table reflects the most accurate and current inventory of managed endpoints.

**QUESTION 11**
A threat intelligence team determines that IP addresses associated with brute force attacks on the VPN gateways are historically linked to a ransomware campaign. Which two features can be defined in Cortex to trigger alerts on the malicious objects and on specified system processes linked to the tactics, techniques, and procedures (TTPs) of the threat actors? (Choose two.)

A. External dynamic list
B. Security event anomaly
C. Behavioral indicator of compromise (BIOC)
D. Indicator of compromise (IOC)

**Answer:** CD
**Explanation:**
Indicators of compromise can be used to detect and alert on known malicious objects such as IP addresses associated with ransomware campaigns. Behavioral indicators of compromise identify suspicious system processes and behaviors linked to attacker tactics, techniques, and procedures, enabling detection of malicious activity patterns beyond static indicators.

**QUESTION 12**
Which operational status will identify all endpoints with agents that are not functioning properly due to insufficient resources?

A. Unprotected
B. Not Protected
C. Limited Protection
D. Local Resource Impact

**Answer:** D
**Explanation:**
Local Resource Impact identifies endpoints where the agent is experiencing performance or functionality issues due to insufficient local system resources, affecting proper operation and protection capability.

**QUESTION 13**
Which Cortex Cloud capability will increase efficiency when prioritizing and categorizing issues?

A. SmartScore
B. Manual tagging
C. SmartGrouping
D. Static threshold

**Answer:** C
**Explanation:**
SmartGrouping increases efficiency by automatically correlating and grouping related issues,

helping security teams prioritize and categorize findings more effectively while reducing alert fatigue and repetitive investigation work.

**QUESTION 14**
A developer writes a serverless application to extract a field from a file in an S3 bucket. The Lambda function is assigned the S3FullAccess managed policy.

```
import requests
...
s3 = boto3.client('s3')

def lambda_handler(event, context):
  bucket = 'userdata'
  key = 'old_user_key_hashes.json'
...
  extracted_fields = {
    'field_name': data.get('API_KEY')
  }
...
```

**Refer to the scenario to answer this question:**

Which two actions will allow a Cortex Cloud user to view the effective permissions of the Lambda function? (Choose two.)

A. Opening the Identity dashboard, filtering for serverless functions, opening the function and clicking on “Access”
B. Viewing all Compute assets and applying the Serverless = Yes filter in the inventory
C. Viewing the Access tab in the non-human identities inventory
D. Selecting the Access tab in the serverless function inventory after selecting the function

**Answer:** CD
**Explanation:**
Effective permissions for a Lambda function can be viewed through the Access tab in the non-human identities inventory and through the Access tab within the serverless function inventory after selecting the function. These views expose the permissions and access relationships associated with the serverless workload.

**QUESTION 15**
Which Cortex Cloud report is most appropriate for a cybersecurity director to receive critical and high compliance risks for AWS?

A. Cloud Risk
B. Asset Inventory
C. Cloud Security Assessment
D. Intelligence Assessment

**Answer:** C
**Explanation:**
The Cloud Security Assessment report provides executive-level visibility into cloud compliance posture, including critical and high compliance risks across AWS environments, making it suitable for cybersecurity leadership review.

**QUESTION 16**
Which feature of Cloud Security Posture Management (CSPM) helps detect and prioritize critical risks in cloud environments?

A. Attack path analysis
B. Vulnerability scanning
C. Compliance checklist
D. Risk assessment

**Answer:** A
**Explanation:**
Attack path analysis helps detect and prioritize critical cloud risks by identifying exploitable paths attackers could use to move through cloud environments, allowing security teams to focus on the most impactful and reachable threats.

**QUESTION 17**
A company has a costly ransomware incident on its Azure infrastructure after an employee was phished while using an unpatched personal computer to download company bank statements. Which two Cloud Security Management modules are most capable of mitigating such incidents and helping the company improve its security posture? (Choose two.)

A. Vulnerability security
B. Data security
C. Application security
D. Identity security

**Answer:** AD
**Explanation:**
Vulnerability security helps identify and remediate unpatched systems that attackers can exploit during ransomware attacks. Identity security strengthens protection against compromised credentials and phishing-based account abuse by monitoring identities, permissions, and risky access behavior.

**QUESTION 18**
What allows Cortex Cloud to provide vulnerability visibility by default upon onboarding cloud service provider (CSP) accounts?

A. Agentless disk scanner
B. Cortex CLI scan
C. Third-party ingestion
D. XDR Cloud agent

**Answer:** A
**Explanation:**
The agentless disk scanner enables Cortex Cloud to automatically discover and assess vulnerabilities across cloud workloads after onboarding CSP accounts, without requiring agents to be installed on the assets.

# 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

**10% Discount Coupon Code:** **ASTR14**