Vendor: Palo Alto Networks

Exam Code: CyberSec-Apprentice

Exam Name: Palo Alto Networks Cybersecurity Apprentice

Version: DEMO

QUESTION 1
Which two technologies will secure a data center's infrastructure from network-based threats? (Choose two.)

A. Next-generation firewall
B. Intrusion Detection System (IDS)
C. Intrusion Prevention System (IPS)
D. Proxy

Answer: AD
Explanation:
A next-generation firewall (NGFW) inspects and controls traffic at the application level to block malicious activity.

An Intrusion Prevention System (IPS) actively detects and blocks network-based threats, protecting the data center infrastructure.

QUESTION 2
Syslog would be used for which activity?

A. Transferring log events within networks
B. Securing endpoints via runtime protection
C. Securing logs collected from endpoints
D. Connecting to a system remotely

Answer: A
Explanation:
Syslog is a standard protocol used to transfer and centralize log events from various devices and systems within a network for monitoring and analysis.

QUESTION 3
What is the primary purpose of an Intrusion Prevention System (IPS)?

A. Detecting malicious traffic before reaching trusted network
B. Filtering malicious traffic before reaching trusted network
C. Building code for server infrastructure
D. Deploying scanners for server infrastructure

Answer: B
Explanation:
An Intrusion Prevention System (IPS) actively monitors network traffic and filters or blocks malicious packets before they reach the trusted network, thereby preventing intrusions in real time.

QUESTION 4
What is a function of an Intrusion Detection System (IDS)?

A. Rejecting connections deemed anomalous
B. Filtering outbound malicious TCP packets
C. Monitoring network traffic for specific patterns

D. Dropping inline network packets

Answer: C
Explanation:
An Intrusion Detection System (IDS) monitors network traffic and analyzes it for specific signatures or behavioral patterns that indicate potential malicious or unauthorized activity.

QUESTION 5
What are two areas in which AI can help Security Operations Center (SOC) teams with alerts? (Choose two.)

A. Vulnerability patching
B. Alert triage
C. SOC resource management
D. Incident response

Answer: BD
Explanation:
AI assists with alert triage by analyzing and prioritizing security alerts to reduce false positives.

AI supports incident response by automating detection, correlation, and recommended remediation actions for faster threat containment.

QUESTION 6
Which concept is a strategic approach to cybersecurity that continuously validates every stage of a digital interaction?

A. Incident response plan implementation
B. Zero Trust adoption
C. Compliance planning
D. Operations playbook development

Answer: B
Explanation:
Zero Trust adoption is a cybersecurity strategy that assumes no user or device is inherently trusted, continuously verifying and validating every stage of digital interaction before granting access.

QUESTION 7
What will cause an unusually high number of false positive alerts?

A. Post-breach recovery plan is well defined.
B. User privilege is configured to be strict.
C. Device is unable to receive an IP address.
D. Traffic match criteria is too generalized.

Answer: D
Explanation:
When traffic match criteria are too generalized, the detection rules trigger on normal network behavior, resulting in an unusually high number of false positive alerts.

QUESTION 8
What is a desired outcome of automation is a security operations center (SOC)?

A. Increased number of alerts
B. Increased MTTR
C. Increased efficiency
D. Increased false positives

Answer: C
Explanation:
Automation in a Security Operations Center (SOC) increases efficiency by streamlining repetitive tasks, accelerating incident response, and reducing manual workload for analysts.

QUESTION 9
Which feature defines a firewall as being next-generation?

A. Application awareness
B. Intrusion prevention
C. Biometric security
D. Static inspection

Answer: A
Explanation:
Application awareness defines a next-generation firewall (NGFW), enabling it to identify, control, and inspect traffic based on specific applications rather than just ports or protocols.

QUESTION 10
What are two characteristics of data loss prevention (DLP)? (Choose two.)

A. Traffic shaping
B. Key logging
C. File-level encryption
D. Content-aware

Answer: CD
Explanation:
File-level encryption protects sensitive data by securing files from unauthorized access.

Content-aware capability enables DLP to inspect and identify sensitive information based on its content to prevent unauthorized transmission.

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**