Boost up Your Certification Score

AI CERTs

AT-510

AI+ NetworkExamination



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.

Visit us at: https://www.examsboost.com/test/at-510

Latest Version: 6.0

Question: 1

How does AI allocate network resources efficiently?

A. By consolidating all traffic into a single channel.
B. By adapting bandwidth usage to real-time traffic needs.
C. By maintaining consistent bandwidth across all devices.
D. By prioritizing data streams based on packet size only.

Answer: B

Explanation:
AI allocates network resources efficiently by adapting bandwidth usage based on real-time traffic conditions. AI+ Network documentation explains that AI-driven systems continuously analyze live telemetry data such as congestion levels, application demand, latency, and packet loss.
Using this data, AI dynamically adjusts bandwidth allocation to ensure that critical applications receive priority while less important traffic is deprioritized during peak usage. This adaptive approach prevents bottlenecks, improves Quality of Service QoS, and enhances overall network performance.
Static bandwidth allocation and single-channel consolidation lack flexibility and fail to respond to dynamic traffic patterns. AI+ Network frameworks emphasize real-time adaptability as the core advantage of AI-driven resource management.

Question: 2

Scenario: A financial services company is experiencing an unusual number of login attempts from different global IP addresses on an employee account. They need to determine whether the account is compromised while ensuring minimum disruption to operations. Which AI-driven security feature would best address this issue?

A. Behavioral analysis to compare current activity with the account's baseline patterns.
B. Static analysis to evaluate metadata associated with the login attempts.
C. Signature-based detection to match activity with known threat databases.
D. Heuristic analysis to apply generalized rules for identifying threats.

Answer: A

Explanation:
Behavioral analysis is the most effective AI-driven security feature for detecting potential account compromise while minimizing operational disruption. AI+ Network security frameworks emphasize behavioral analysis as a technique that establishes a baseline of normal user behavior , including login locations, times, devices, and access patterns.

When deviations occur—such as simultaneous or rapid login attempts from multiple global IP addresses—the AI system flags the activity as anomalous without immediately blocking access. This allows security teams to investigate potential compromise while maintaining business continuity. Unlike signature-based detection, which only identifies known threats, behavioral analysis can detect previously unseen or zero-day attack patterns .
Static and heuristic analyses are less precise in this context, as they rely on predefined rules or metadata rather than adaptive learning. Financial institutions, in particular, benefit from behavioral AI because it balances security, accuracy, and user experience , reducing false positives and unnecessary lockouts.

Question: 3

What functionality does Bubbln provide to enhance network management?

A. Automates routine network tasks and configurations efficiently.
B. Provides deep learning models for DNS domain classification.
C. Offers penetration testing for identifying vulnerabilities.
D. Deploys ML models for anomaly detection in real-time.

Answer: A

Explanation:
Bubbln enhances network management by automating routine network tasks and configuration processes. AI+ Network automation documentation describes Bubbln as an orchestration-focused platform designed to reduce manual intervention in repetitive network operations such as provisioning, configuration updates, compliance checks, and policy enforcement.
By automating these tasks, Bubbln improves operational efficiency, reduces human error, and ensures configuration consistency across large-scale network environments. This is particularly valuable in enterprise and multi-cloud infrastructures where managing devices manually becomes complex and error-prone.
Unlike tools focused on security analytics, penetration testing, or anomaly detection, Bubbln's primary role is workflow automation and orchestration . AI+ Network materials emphasize automation platforms like Bubbln as critical enablers of scalable, agile, and AI-ready networks, allowing engineers to focus on optimization and strategic initiatives rather than repetitive tasks.

Question: 4

What distinguishes Cisco Packet Tracer from GNS3 in terms of usability?

A. It integrates with third-party virtualization tools like VMware.
B. It supports real network operating systems for precise emulation.
C. It focuses on enterprise-grade networking scenarios exclusively.
D. It offers a user-friendly interface designed for Cisco device simulations.

Answer: D

Explanation:

Cisco Packet Tracer is distinguished by its user-friendly interface specifically designed for simulating Cisco networking devices. AI+ Network lab documentation highlights Packet Tracer as an educational tool aimed at beginners and intermediate learners, providing intuitive drag-and-drop topology creation and simplified configuration workflows.
Unlike GNS3, which runs real network operating systems and requires greater system resources and expertise, Packet Tracer uses simulated devices with guided configuration support. This makes it ideal for learning foundational networking concepts, practicing CCNA-level labs, and visualizing packet flow without complex setup.
Packet Tracer does not integrate with virtualization platforms like VMware and does not support real IOS images. AI+ Network materials emphasize Packet Tracer's accessibility and ease of use as its primary advantage over more advanced emulation tools.

Question: 5

Which system is best for detecting unauthorized logins and adapting to new threats?

A. Static firewalls
B. Load balancers
C. Reactive AI
D. Machine learning-driven intrusion detection

Answer: D

Explanation:
Machine learning–driven intrusion detection systems IDS are best suited for detecting unauthorized logins and adapting to emerging threats. AI+ Network security documentation highlights ML-driven IDS as systems that continuously learn from historical and real-time data to identify abnormal behavior. Unlike static firewalls, which rely on predefined rules, ML-based IDS can detect novel attack patterns, brute-force attempts, and compromised credentials. They adapt over time, improving detection accuracy and reducing false positives.
Load balancers are unrelated to security monitoring, and reactive AI responds after incidents rather than proactively detecting them. AI+ Network materials consistently identify machine learning–driven IDS as a core component of modern, adaptive cybersecurity architectures.

Question: 6

How are devices within a VNET able to communicate with devices on other networks?

A. By setting up routing protocols for path selection.
B. By configuring NAT rules for external routing.
C. By defining IP address boundaries and subnets.
D. By using Layer 2 switching for traffic forwarding.

Answer: A

Explanation:

Devices within a Virtual Network VNET communicate with devices on other networks through routing mechanisms that determine the best path for traffic. AI+ Network foundational networking documents explain that routing protocols or static routing configurations enable Layer 3 connectivity between separate IP networks.

Routing protocols such as OSPF, BGP, or static routes allow routers and virtual gateways to exchange network reachability information. This ensures that packets can traverse different network segments, cloud regions, or on-premise environments. Without routing, devices would be limited to local subnet communication only.

NAT may be used for address translation but does not itself enable network-to-network communication. Defining IP subnets establishes network boundaries but does not provide connectivity. Layer 2 switching operates within the same broadcast domain and cannot forward traffic across different networks.

AI+ Network training materials consistently reinforce that routing is the core mechanism enabling inter-network communication in both physical and virtualized environments.

Visit us at: https://www.examsboost.com/test/at-510

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

