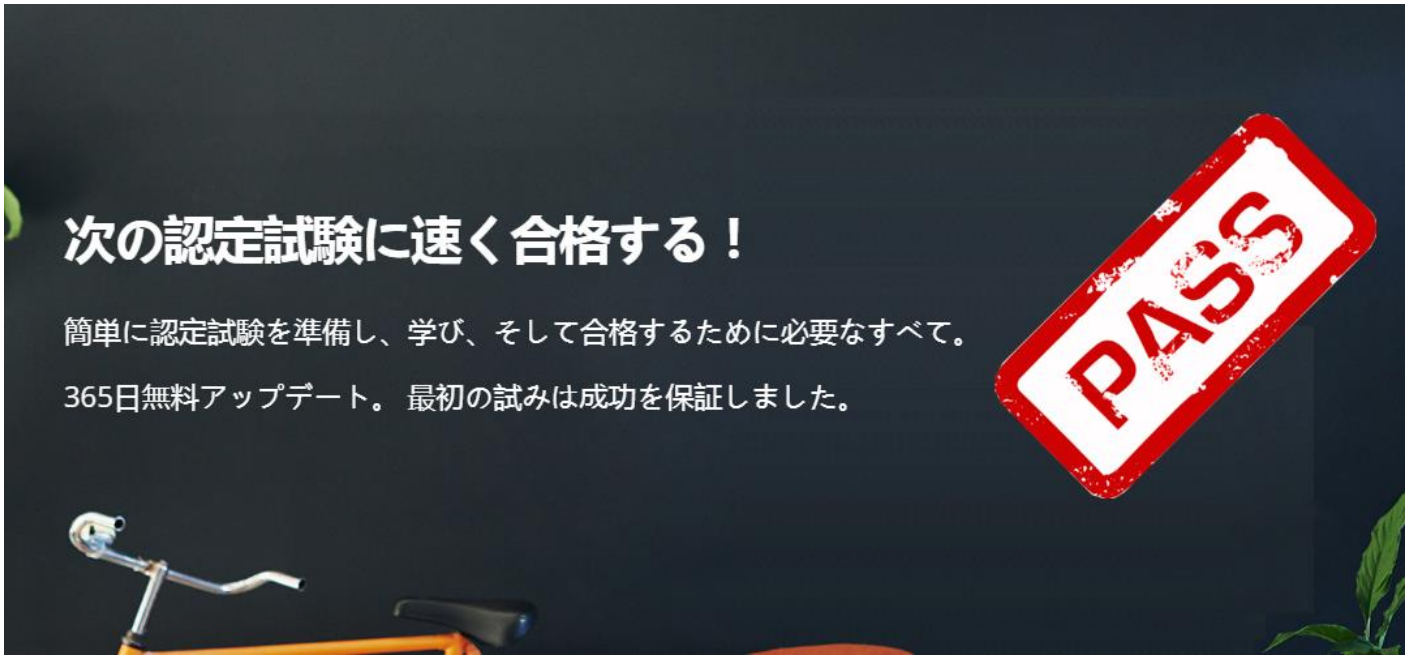
PASSTEST
いつでも試験に合格して

PASSTEST



インスタントダウンロード

お支払い後、弊社のシステムは、1分以内に購入した商品をあなたのメールボックスにお送りします。 2時間以内に届かない場合に、お問い合わせください。

365日無料アップデート

購入日から365日無料アップデートをご利用いただけます。365日後、更新版がほしく続けて50%の割引を与えれます。

返金保証

購入後60日以内に、試験に合格しなかった場合は、全額返金します。そして、無料で他の製品を入手できます。

セキュリティ&プライバシー

我々は顧客のプライバシーを尊重する。McAfeeセキュリティ サービスを使用して、お客様の個人情報および安心のために最大限のセキュリティ を提供します。

https://www.passtest.jp/

高質量の国際認定試験問題集の提供者、試験に合格させろう！

Exam : **AT-510**

Title : AI+ NetworkExamination

Vendor : AI CERTs

Version : DEMO

NO.1 (Why is GNS3 considered superior for advanced network emulation compared to simpler simulators?)

A. It supports real operating systems for realistic network behavior.

B. It focuses on simulating Cisco devices.

C. It requires minimal system resources for complex scenarios.

D. It provides a pre-configured environment for basic networking tasks.

Answer: A

Explanation:

GNS3 is considered superior for advanced network emulation because it supports real network operating systems, providing highly realistic network behavior. According to AI+ Network lab documentation, GNS3 allows engineers to run actual router and switch images, including Cisco IOS, IOS-XE, JunOS, and Linux- based systems, rather than relying on simplified simulations.

This capability enables accurate testing of routing protocols, security features, automation scripts, and failure scenarios exactly as they would behave in production environments. Unlike basic simulators, GNS3 does not abstract protocol behavior, making it ideal for advanced troubleshooting, certification labs, and enterprise network design validation.

While GNS3 can simulate Cisco devices, it is not limited to them. It also requires more system resources, not fewer, due to its realism. Pre-configured environments are typically associated with beginner tools, whereas AI+ Network training emphasizes GNS3 for advanced, real-world emulation and hands-on skill development.

NO.2 (How does DeepSlice enhance 5G network slicing?)

A. By using deep learning to optimize load management.

B. By focusing on static DNS domain classifications.

C. By automating penetration testing for security vulnerabilities.

D. By preemptively blocking threats to web applications and APIs.

Answer: A

Explanation:

DeepSlice enhances 5G network slicing by applying deep learning techniques to optimize load management across network slices. AI+ Network documentation explains that 5G slicing allows multiple virtual networks to operate on the same physical infrastructure, each tailored to specific service requirements such as latency, bandwidth, or reliability.

DeepSlice continuously analyzes traffic demand, user mobility, and application performance metrics. Using deep learning models, it dynamically adjusts resource allocation to ensure each slice receives the appropriate level of service. This improves efficiency, reduces congestion, and maintains Quality of Service (QoS) for diverse use cases such as autonomous vehicles, IoT, and enhanced mobile broadband.

Other options relate to security or DNS analysis and do not address slice optimization. AI+ Network materials identify DeepSlice as a critical innovation for intelligent, adaptive 5G resource management.

NO.3 (What is the purpose of VLANs in a network?)

A. To enhance physical connectivity between devices.

B. To logically divide a physical network into isolated segments.

C. To provide internet access to all connected devices.

D. To replace the need for network switches and routers.

Answer: B

Explanation:

Virtual Local Area Networks (VLANs) are used to logically divide a single physical network into multiple isolated broadcast domains. According to AI+ Network foundational documentation, VLANs allow network administrators to group devices based on function, department, or security requirements rather than physical location.

By segmenting a network logically, VLANs improve security by limiting broadcast traffic and reducing the scope of potential attacks. Devices in different VLANs cannot communicate directly without routing, which allows administrators to enforce access control policies. VLANs also enhance performance by reducing unnecessary broadcast traffic across the entire network.

VLANs do not enhance physical connectivity, provide internet access by themselves, or replace networking hardware. Instead, they work in conjunction with switches and routers to create scalable, secure, and efficient network architectures. AI+ Network materials consistently identify VLANs as a core technique for network segmentation and traffic management.

NO.4 (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.

Question: 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 abaseline 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 detectpreviously 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.

NO.5 (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.