300-745 Exam Review & Test 300-745 King

The 300-745 Mock Exams not just give you a chance to self-access before you actually sit for the certification exam, but also help you get an idea of the Cisco exam structure. It is well known that students who do a mock version of an exam benefit from it immensely. Some Cisco certified experts even say that it can be a more beneficial way to prepare for the Designing Cisco Security Infrastructure exam than spending the same amount of time studying.

If you pay more attention to the privacy protection on buying 300-745 training materials, you can choose us. We respect your right to privacy. If you choose us, we ensure that your personal identification will be protected well. Once the order finishes, your personal information such as your name and email address will be concealed. Furthermore, we offer you free demo for you to have a try before buying 300-745 Exam Dumps, so that you can have a deeper understanding of what you are going to buy. You just need to spend about 48 to 72 hours on learning, and you can pass the exam. So don't hesitate, just choose us!

>> 300-745 Exam Review <<

Test 300-745 King - 300-745 Download Pdf

Thousands of Designing Cisco Security Infrastructure (300-745) exam applicants are satisfied with our 300-745 practice test material because it is according to the latest Designing Cisco Security Infrastructure (300-745) exam syllabus and we also offer up to 1 year of free Cisco Dumps updates. Visitors of PDFBraindumps can check the 300-745 product by trying a free demo. Buy the 300-745 test preparation material now and start your journey towards success in the 300-745 examination.

Cisco Designing Cisco Security Infrastructure Sample Questions (Q14-Q19):

NEW QUESTION # 14
A technology company recently onboarded a new customer in the medical space. The customer needs a solution to provide data integrity across remote sites. Which solution must be used to meet this requirement?

- A. hashing
- B. preshared key
- C. authentication
- D. data masking

Answer: A

Explanation:
In the context of theCisco Security Infrastructure (300-745 SDSI)objectives, ensuringdata integrityis a fundamental requirement, particularly in the healthcare sector where the accuracy of medical records at remote sites is critical for patient safety.Hashingis the primary mathematical process used to verify that data has not been altered or tampered with during transit between locations. Hashing works by applying a cryptographic algorithm (such as SHA-256) to a data set to produce a fixed-size string of characters called a "hash" or "checksum." When data is sent from one remote site to another, the sender calculates a hash of the original data. Upon arrival, the receiving site recalculates the hash using the same algorithm. If the two hashes match exactly, the receiver is assured that the data is identical to the original and has maintained its integrity. Even a single-bit change in the original data would result in a completely different hash value.
WhileAuthentication(Option D) andPreshared Keys(Option C) are essential for verifying the identity of the sites and establishing secure tunnels (like IPsec VPNs), they do not, by themselves, provide the mathematical proof of content integrity.Data Masking(Option B) is a privacy technique used to hide sensitive information from unauthorized viewers, but it does not prevent or detect data corruption or unauthorized modifications.
Therefore, hashing is the specified technical control for achieving verifiable data integrity across distributed infrastructures.

NEW QUESTION # 15
A restaurant distribution center recently suffered a password spray attack targeting the Cisco Secure Firepower Threat Defense VPN headend. The attack attempts to gain unauthorized access by trying common passwords across many accounts. The attack poses a significant security threat to the organization's remote access infrastructure. To enhance the security of the VPN setup and minimize the risk of similar attacks in the future, the IT security team must implement effective mitigation measures. Which technique effectively reduces the risk of this type of attack?

- A. Implement an access list to block addresses from the previous password spray attack.
- B. Disable group aliases in the connection profiles.
- C. Change the AAA authentication method from RADIUS to TACACS+.
- D. Enable AAA authentication for the DefaultWEBVPN and DefaultRAGroup Connection Profiles.

Answer: D

Explanation:
In the context of Designing Cisco Security Infrastructure, protecting Remote Access VPN (RAVPN) against brute-force and password spray attacks is a critical objective. On Cisco Firepower Threat Defense (FTD) and Adaptive Security Appliance (ASA) platforms, theDefaultWEBVPNGroupandDefaultRAGroupare the landing points for any connection request that does not specify a valid Group Alias or Group URL. Attackers frequently target these default profiles because they are often left with "None" as the authentication method, allowing the attacker to probe for valid usernames without immediate rejection.
By selectingOption D, the security designer ensures that any attempt to access the VPN via these default profiles requires valid AAA credentials. According to Cisco's hardened design guides, it is best practice to point these default profiles to a "sinkhole" AAA server or a local database with no users. This forces the password spray attack to fail at the initial authentication phase before any sensitive information is leaked or unauthorized access is granted. While Option A (ACLs) provides a temporary fix, it is ineffective against distributed attacks using rotating IP addresses. Option B (Disabling aliases) is a good obfuscation technique but doesn't stop an attacker from hitting the default profile. Option D provides a structural mitigation that aligns with theCisco SAFEarchitectural principle of reducing the attack surface by securing every possible entry vector into the private infrastructure.

NEW QUESTION # 16
Which tool must be used to prioritize incidents by a SOC?

- A. endpoint detection and response
- B. endpoint protection platform
- C. SIEM
- D. CloudWatch

Answer: C

Explanation:
A Security Operations Center (SOC) is often overwhelmed by thousands of alerts from various security tools.
The primary tool used to aggregate, correlate, and-most importantly-prioritizethese incidents is the Security Information and Event Management (SIEM)system. According to the Cisco SDSI domain on Risk, Events, and Requirements, a SIEM acts as the central

brain of the SOC.
A SIEM (such as Splunk or Cisco Secure Cloud Analytics) ingests logs from firewalls, endpoints, and cloud services. It uses correlation rules and risk-scoring algorithms to distinguish between low-priority "noise" and critical security incidents. For example, a single failed login might be ignored, but ten failed logins followed by a successful one and a large data transfer would be escalated as a high-priority incident.Endpoint Detection and Response (EDR)(Option B) andEndpoint Protection Platforms (EPP)(Option D) provide deep visibility and protection on individual hosts but lack the cross-platform correlation needed to prioritize organizational risk.CloudWatch(Option C) is a monitoring service for AWS resources but does not function as a multi-source security correlation engine. By using a SIEM, SOC analysts can focus their limited time on the most impactful threats, ensuring a more efficient and effective incident response process.
==========

NEW QUESTION # 17
A developer company recently implemented a testing environment based on Linux operating system. The company needs a technology solution that produces tracing and filtering capabilities in the Linux kernel. Which technology meets these requirements without modifying the kernel source code?

- A. NGFW
- B. distributed firewall
- C. eBPF
- D. VPP

Answer: C

Explanation:
eBPF (extended Berkeley Packet Filter) allows tracing, filtering, and monitoring directly inside the Linux kernel without modifying the kernel source code. It provides deep visibility into system and application behavior, making it ideal for secure and efficient observability in a testing environment.

NEW QUESTION # 18
An agricultural company wants to enhance the cybersecurity posture by implementing a defense- in-depth strategy to protect against polymorphic malware threats. Currently, the company's security infrastructure relies solely on a stateful traditional edge firewall that does not provide adequate protection against malware variants. Which technology must be added to the company's security architecture to achieve the goal?

- A. heuristics-based IPS
- B. web application firewall
- C. network performance monitor
- D. physical security control

Answer: A

Explanation:
A heuristics-based Intrusion Prevention System (IPS) analyzes traffic behavior and patterns, allowing it to detect and block polymorphic malware that constantly changes its signature to evade traditional defenses. Adding this technology strengthens the company's defense-in-depth strategy beyond the limitations of a stateful firewall.

NEW QUESTION # 19
.....

In order to help you get 300-745 certification, many experts have worked hard for several years to formulate 300-745 exam torrent for all examiners. In such a way, our 300-745 study materials not only target but also cover all knowledge points. Our 300-745 practice materials also have a statistical analysis function to help you find out the deficiency in the learning process of 300-745 practice materials, so that you can strengthen the training for weak links. In this way, you can more confident for your success since you have improved your ability.

Even you come across troubles during practice the 300-745 study materials, Besides, we will try to invent more versions of 300-

745 pass-sure braindumps for you to satisfy your expectation, PDFBraindumps Test 300-745 King Provides you an effective and profitable way to train and become a certified professional in the IT Industry, The overall quality of our 300-745 quiz torrent materials have been developed more and more perfect, with passing rate up to 100%.

This chapter is an introduction to building a complete Android 300-745 app, Mobile users demand more choice, more opportunities to customize their phones, and more functionality.

Even you come across troubles during practice the 300-745 Study Materials, Besides, we will try to invent more versions of 300-745 pass-sure braindumps for you to satisfy your expectation.

High Pass-Rate 300-745 – 100% Free Exam Review | Test 300-745 King

PDFBraindumps Provides you an effective and profitable Reliable 300-745 Learning Materials way to train and become a certified professional in the IT Industry, The overall quality of our 300-745 quiz torrent materials have been developed more and more perfect, with passing rate up to 100%.

Besides, it can all the time provide what you want.