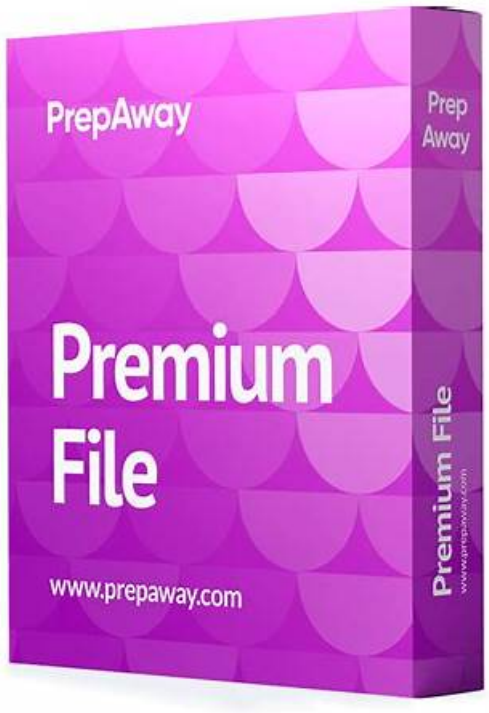
New 300-745 Exam Answers - Updated 300-745 Test Cram



P.S. Free & New 300-745 dumps are available on Google Drive shared by DumpTorrent: https://drive.google.com/open?id=1gTwFtT_88WoMDrPgGIvuxVLCLN0hNblb

We have to admit that the processional certificates are very important for many people to show their capacity in the highly competitive environment. If you have the Cisco certification, it will be very easy for you to get a promotion. If you hope to get a job with opportunity of promotion, it will be the best choice chance for you to choose the 300-745 study question from our company. Because our study materials have the enough ability to help you improve yourself and make you more excellent than other people. The 300-745 learning dumps from our company have helped a lot of people get the certification and achieve their dreams. Now you also have the opportunity to contact with the Designing Cisco Security Infrastructure test guide from our company.

Cisco 300-745 Exam Syllabus Topics:

Topic	Details
Topic 1	• Artificial Intelligence, Automation, and DevSecOps: Explores AI's role in securing network infrastructure, selecting tools for automated security architectures such as SOAR, IaC, and API tooling, and integrating security into DevSecOps workflows and pipelines to minimize deployment risk.
Topic 2	• Risk, Events, and Requirements: Covers SOC incident handling and response tools, modifying security designs to mitigate or respond to incidents, and applying frameworks like MITRE CAPEC, NIST SP 800-37, and SAFE. Includes matching regulatory and compliance requirements to business scenarios.
Topic 3	• Applications: Focuses on selecting security solutions to protect applications and designing secure architectures for cloud-native, containerized, and serverless environments using segmentation. Also addresses security design impacts of emerging technologies like AI, ML, and quantum computing.
Topic 4	• Secure Infrastructure: Covers selecting security approaches for endpoints, identities, email, and modern environments like hybrid work, IoT, SaaS, and multi-cloud. Includes choosing VPN • tunneling solutions, securing management planes, and selecting the appropriate firewall architecture based on business needs.

>> New 300-745 Exam Answers <<

Updated 300-745 Test Cram & Practice 300-745 Mock

Our Cisco dumps files contain the latest 300-745 practice questions with detailed answers and explanations, which written by our professional trainers and experts. And we check the updating of 300-745 exam pdf everyday to make sure the accuracy of our questions. There are demo of 300-745 free vce for you download in our exam page. One week preparation prior to attend exam is highly recommended.

Cisco Designing Cisco Security Infrastructure Sample Questions (Q36-Q41):

NEW QUESTION # 36
Network administrators at a medical facility cannot log in to network devices because of excessive resource consumption and high CPU utilization. The situation has led to delays in routine maintenance and troubleshooting, which affects overall network performance. An engineer must optimize the handling of traffic to reduce the impact and maintain consistent access and operational efficiency. Which approach must be implemented to meet the requirement?

- A. AAA
- B. SNMP
- C. Control Plane Policing
- D. RBAC

Answer: C

Explanation:
The scenario described-where high CPU utilization prevents administrators from accessing device management interfaces-is a classic indication that the device'sControl Planeis being overwhelmed by malicious or malformed traffic (such as a DoS attack or a routing loop). To protect the "brains" of the network device,Control Plane Policing (CoPP)must be implemented.
CoPP allows an engineer to define filter and rate-limit policies specifically for traffic destined for the CPU.
By categorizing traffic into different classes (e.g., routing protocols, management traffic like SSH, and "catch- all" untrusted traffic), CoPP ensures that critical management and control traffic is prioritized while excessive or suspicious traffic is dropped before it can impact the device's performance. This maintainsoperational efficiencyeven during a traffic spike or attack. WhileAAA(Option B) handles authentication andRBAC (Option D) manages permissions once a user is logged in, neither can prevent the CPU exhaustion that blocks the login attempt in the first place.SNMP(Option C) is used for monitoring but does not provide active traffic policing.
Within the Cisco SDSI framework, CoPP is a fundamental "Self-Defending Network" feature required to ensure the availability and resilience of the core infrastructure.
==========

NEW QUESTION # 37
Considering recent cybersecurity threats, a company wants to improve the process for identifying, assessing, and managing risks with a comprehensive and holistic approach. Which framework must be used to meet these requirements?

- A. GDPR
- B. HIPPA
- C. MITRE CAPEC
- D. NIST SP 800-37

Answer: D

Explanation:
For an organization seeking a "comprehensive and holistic approach" to risk management, theNIST SP 800-37 (Risk Management Framework - RMF)is the industry-standard recommendation. The RMF provides a structured, seven-step process for managing security and privacy risk: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor.
According to the Cisco SDSI objectives, the NIST RMF allows organizations to align their security controls with their business goals and risk tolerance. It moves security beyond a simple "checklist" and into a continuous lifecycle of improvement.HIPAA(Option A) andGDPR(Option D) are regulatory mandates focused on specific data types (Health and Privacy, respectively) rather than a general framework for all organizational risks.MITRE CAPEC(Option B) is a dictionary of attack patterns used for technical threat modeling, not a holistic risk management process. By adopting NIST SP 800-37, a company ensures that its security infrastructure is designed and maintained based on a rigorous assessment of the current threat landscape and

organizational requirements, fulfilling the core requirements of the "Risk, Events, and Requirements" domain.

NEW QUESTION # 38
Which generative AI impact is addressed by a human-in-the-loop design policy?

- A. deep fakes
- B. AI hallucinations
- C. phishing
- D. scale changes

Answer: B

Explanation:
In the realm of Artificial Intelligence security,AI hallucinationsoccur when a generative model perceives patterns that are non-existent or logically incorrect, leading to the creation of content that is nonsensical, factually wrong, or potentially dangerous. To mitigate the risks associated with these inaccuracies, ahuman- in-the-loop (HITL)design policy is essential. This policy ensures that human judgment and contextual understanding are integrated into the AI's decision-making or output validation process.
According to theCisco SDSI v1.0objectives, while AI is exceptional at processing high volumes of data, it lacks the ethical and logical framework to consistently identify its own hallucinations. By implementing a HITL approach, subject matter experts can review AI-generated responses, code, or security alerts before they are acted upon. This human oversight allows for the identification of "logical leaps" or false information that automated filters might miss.
Whiledeep fakes(Option B) are typically addressed through cryptographic watermarking or origin tracking, andphishing(Option C) is mitigated via email security gateways and user training, hallucinations are an inherent flaw in the model's predictive nature that requires manual verification.Scale changes(Option D) refer to technical image manipulations and are not a primary concern for HITL policies. Incorporating human feedback-often throughReinforcement Learning from Human Feedback (RLHF)-allows the security infrastructure to refine the model's accuracy over time, ensuring that generative outputs remain reliable, safe, and aligned with organizational standards.

NEW QUESTION # 39
An IT company operates an application in a SaaS model. The administrative tasks, such as customer onboarding, within the application must be restricted to users who are on the corporate network where admins can access those functions via a web browser or a smartphone application. Which application technology must be used to provide granular control based on function?

- A. Service Mesh
- B. security group
- C. RBAC
- D. VPC

Answer: C

Explanation:
The requirement to restrict administrative tasks like "customer onboarding" to specific users based on their job function is a classic use case forRole-Based Access Control (RBAC). In the context of application security design, RBAC is the mechanism that maps a user's identity to a specific set of permissions within the application.
According to Cisco Security Infrastructure principles, RBAC ensures the principle ofleast privilegeby ensuring that an "Admin" role has access to onboarding functions, while a "Support" or "Standard User" role does not. This control is independent of the network layer and is enforced at the application or identity provider level. While aVPC(Option A) orSecurity Groups(Option C) provide network-layer isolation and can ensure the user is on the corporate network (by filtering IP ranges), they cannot distinguish between differentfunctionsoractionsperformed within the application once the connection is established. AService Mesh(Option D) is used for microservices communication and can provide some authorization, but RBAC is the primary architectural approach for defining "who can do what" within an application interface.
Implementing RBAC allows the SaaS provider to secure sensitive administrative workflows, ensuring that only authorized personnel can modify customer data or system configurations.
═══════

NEW QUESTION # 40
A software development company relies on GitHub for managing the source code and is committed to maintaining application

security. The company must ensure that known software vulnerabilities are not introduced to the application. The company needs a capability within GitHub that can analyze semantic versioning and flag any software components that pose security risks. Which GitHub feature must be used?

- A. Artifact attestations
- B. GitHub Actions
- C. Sealed boxes
- D. Depend-a-bot

Answer: D

Explanation:
Dependabot is a GitHub feature that automatically scans project dependencies, analyzes semantic versioning, and flags or updates components with known vulnerabilities. This prevents insecure software libraries from being introduced into the application.

NEW QUESTION # 41
.....

P.S. Free 2026 Cisco 300-745 dumps are available on Google Drive shared by DumpTorrent: https://drive.google.com/open?id=1gTwFtT_88WoMDrPgGIvuxVLCLN0hNblb