Valid Braindumps 300-745 Ebook & Reliable 300-745 Exam Registration

BTW, DOWNLOAD part of Prep4away 300-745 dumps from Cloud Storage: https://drive.google.com/open?id=16stZbUKHb92tLgQLDZoFRi5nf5lN-X8Q

The 300-745 practice materials are a great beginning to prepare your exam. Actually, just think of our 300-745 practice materials as the best way to pass the exam is myopic. They can not only achieve this, but ingeniously help you remember more content at the same time. It is estimated conservatively that the passing rate of the exam is over 98 percent with our 300-745 Study Materials as well as considerate services. We not only provide all candidates with high pass rate study materials, but also provide them with good service.

Cisco 300-745 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.

Topic 2	• 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 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	• 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.

Cisco 300-745 Questions PDF File

If you are still hesitate to choose our Prep4away, you can try to free download part of Cisco 300-745 exam certification exam questions and answers provided in our Prep4away. So that you can know the high reliability of our Prep4away. Our Prep4away will be your best selection and guarantee to pass Cisco 300-745 Exam Certification. Your choose of our Prep4away is equal to choose success.

Cisco Designing Cisco Security Infrastructure Sample Questions (Q48-Q53):

NEW QUESTION # 48
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 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. Change the AAA authentication method from RADIUS to TACACS+.
- B. Implement an access list to block addresses from the previous password spray attack.
- C. Disable group aliases in the connection profiles.
- D. Enable AAA authentication for the DefaultWEBVPN and DefaultRAGroup Connection Profiles.

Answer: D

Explanation:
Enabling AAA authentication on the default connection profiles ensures that all VPN access attempts must go through strong authentication. This directly mitigates password spray attacks by enforcing centralized authentication controls, enabling account lockout, and supporting additional protections such as multifactor authentication.

NEW QUESTION # 49
A global energy company moved a monolithic application from the data center to public cloud. Over time, the company added many capabilities to the application, and it is now difficult for the application team to scale it.
The application owner decided to modernize the application by moving to a Kubernetes cluster. However, he wants to ensure that the new application architecture provides a container network interface that is scalable, offers options for cloud-native security, and helps with visibility and observability. Which solution must be used to accomplish the task?

- A. ENI
- B. Cilium
- C. ingress gateway
- D. security group

Answer: B

Explanation:

In the realm of modern application security and Kubernetes networking,Ciliumhas emerged as the industry- standardContainer Network Interface (CNI)that leverageseBPF (extended Berkeley Packet Filter) technology. For a global company modernizing a monolithic app into microservices, Cilium provides the required scalability and high-performance networking by operating directly within the Linux kernel.
Unlike traditionalSecurity Groups(Option A) which are often limited to IP-based rules at the cloud infrastructure level, orENIs(Option C) which are AWS-specific hardware interfaces, Cilium providesidentity- awaresecurity. It understands Kubernetes labels and metadata, allowing for granular Layer 7 policy enforcement. Furthermore, Cilium addresses the "visibility and observability" requirement through itsHubble component, which provides deep insights into network flows, application dependencies, and security events without the overhead of traditional sidecar proxies. AnIngress Gateway(Option D) manages external traffic entering the cluster but does not provide the comprehensive pod-to-pod networking, eBPF-based security, or internal observability that a CNI like Cilium offers. Designing with Cilium aligns with Cisco's focus on cloud- native security and the use of eBPF for distributed firewalling and telemetry in modern application environments.
==========

NEW QUESTION # 50
How does a SOC leverage flow collectors?

- A. It performs load balancing capabilities across systems to optimize performance.
- B. It performs data backup and recovery.
- C. It provides real time content filtering.
- D. It provides data for analysis in threat detection and response system.

Answer: D

Explanation:
A flow collector gathers metadata about network traffic (such as NetFlow or IPFIX), which SOC analysts use to analyze communication patterns. This data is critical for threat detection and response, helping identify anomalies, lateral movement, or potential attacks.

NEW QUESTION # 51
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:
In modern DevSecOps, managing third-party dependencies is a major security challenge.Dependabot(often stylized as Depend-a-bot) is the specific GitHub feature designed to automate the identification and updating of vulnerable dependencies. It works by scanning the application's manifest files (like package.json or requirements.txt) and analyzing thesemantic versioningof the included libraries.
When a known vulnerability (CVE) is reported in a specific version of a library used by the application, Dependabot flags the security risk and alerts the development team. Most importantly, it can automatically generate pull requests to upgrade the dependency to the minimum secure version that resolves the vulnerability. This ensures that the application remains secure without requiring manual tracking of every third-party component.
WhileGitHub Actions(Option C) can be used to run security scanners (like SAST tools), it is a general automation framework, not a dedicated dependency analysis tool.Artifact attestations(Option D) are used to prove the provenance and integrity of a build, andSealed boxes(Option B) is not a standard GitHub security feature related to vulnerability scanning. Utilizing Dependabot directly supports the Cisco SDSI objective of
"Securing the CI/CD pipeline" by proactively managing the Software Bill of Materials (SBOM) and ensuring that vulnerable components do not reach the production environment.

NEW QUESTION # 52
In preparation for an upcoming security audit, a metal production company decided to enhance the security of container-based services running in a Kubernetes environment. The company wants to ensure that all communications between applications and services are encrypted. The administrator plans to implement mTLS service between application and services to secure the data exchanges. Given the need to manage encryption at scale and maintain efficient communication across the cluster, which network transport technology must be employed?

- A. load balancing
- B. ingress controller
- C. Service Mesh
- D. Kubernetes network policies

Answer: C

Explanation:
A Service Mesh provides built-in support for mutual TLS (mTLS) between microservices, ensuring encrypted communication at scale in Kubernetes environments. It also centralizes management of certificates, keys, and security policies, making it the right choice for securing data exchanges across the cluster.

NEW QUESTION # 53
.....

For most IT workers, having the aspiration of getting Cisco certification are very normal, passing 300-745 actual test means you have chance to enter big companies and meet with extraordinary people from all walks of life. The 300-745 Real Questions from our website are best study materials for you to clear exam in a short time.