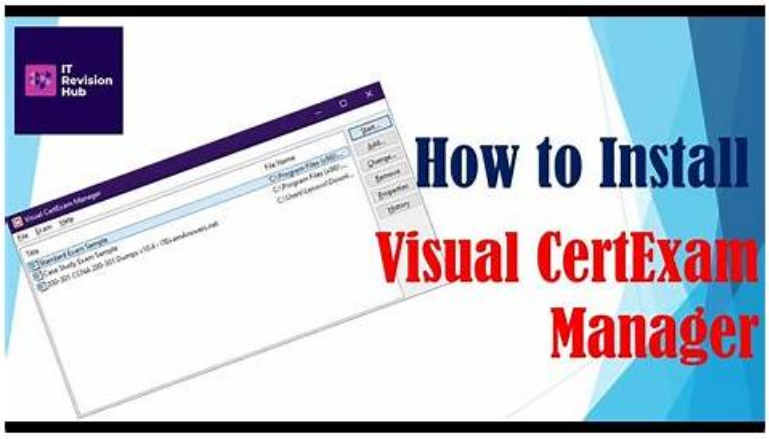
300-745 Detail Explanation, 300-745 Visual Cert Exam



P.S. Free 2026 Cisco 300-745 dumps are available on Google Drive shared by Real4dumps: https://drive.google.com/open?id=1Va9OLHtEn4z0dV_kskJBOCa2LQf6k23p

We hope you can find the information you need at any time while using our 300-745 study materials. In addition to the content updates, our system will also be updated for the 300-745 training materials. If you have any opinions, you can tell us that our common goal is to create a product that users are satisfied with. We have three different 300-745 Exam Braindumps for you to choose: the PDF, Software and APP online. And the varied displays can help you study at any time and condition.

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	• 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 3	• 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 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.

>> 300-745 Detail Explanation <<

300-745 Visual Cert Exam | Valid Exam 300-745 Registration

A Designing Cisco Security Infrastructure (300-745) practice questions is a helpful, proven strategy to crack the Designing Cisco Security Infrastructure (300-745) exam successfully. It helps candidates to know their weaknesses and overall performance. Real4dumps software has hundreds of Designing Cisco Security Infrastructure (300-745) exam dumps that are useful to practice in real-time.

Cisco Designing Cisco Security Infrastructure Sample Questions (Q49-Q54):

NEW QUESTION # 49
A video game company identified a potential threat of a SYN flood attack, which could disrupt the online gaming services and impact user experience. The attack can overwhelm network resources by exploiting the TCP handshake process, leading to server unavailability and degraded performance. To safeguard the company's infrastructure and ensure uninterrupted service, it is essential to enhance the security measures in place. The company must implement a solution that manages and mitigates the risk of such network-based attacks. Which security product must be implemented to mitigate similar risks?

- A. Cisco Web Security Appliance
- B. Cisco Umbrella
- C. Cisco Secure Firewall
- D. Cisco Secure Endpoint

Answer: C

Explanation:
A SYN flood attack is a classic Denial-of-Service (DoS) technique that exploits the TCP three-way handshake. By sending a massive volume of SYN packets without completing the handshake, the attacker exhausts the target server's connection table.Cisco Secure Firewall(formerly Firepower) is the architectural component designed to mitigate these network-layer threats.
Cisco Secure Firewall utilizes features such asTCP InterceptandSYN Cookiesto defend against these attacks. When a SYN flood is detected, the firewall can act as a proxy for the handshake, only passing the completed connection to the backend server once the three-way handshake is verified. This prevents the server's resources from being overwhelmed by "half-open" connections.
In contrast,Cisco Web Security Appliance(Option A) is focused on web-based (HTTP/HTTPS) threats and proxying, not low-level TCP flood mitigation.Cisco Umbrella(Option B) primarily provides DNS-layer security and Secure Internet Gateway (SIG) services, which are ineffective against a direct SYN flood targeting an on-premises or cloud-hosted gaming server.Cisco Secure Endpoint(Option C) protects individual hosts from malware but cannot protect the network infrastructure or the server's TCP stack from being saturated by high-volume flood traffic. Consequently, Cisco Secure Firewall is the essential product for managing and mitigating these infrastructure-level network attacks.
==========

NEW QUESTION # 50
A company published software that had a security vulnerability, and an attacker used the vulnerability to steal critical information from the environment. The issue was reported by the security team, and the administrator was instructed to run shift-left security tests before publishing the software. Which component of the software development pipeline must be recommended to run the tests?

- A. cloud security posture management
- B. software bill of material analysis
- C. source code management
- D. continuous deployment

Answer: C

Explanation:
Shift-left security means running security tests earlier in the development lifecycle. By integrating tests in the source code management stage (e.g., Git repositories), vulnerabilities can be detected and fixed before software is built and deployed, reducing the risk of publishing insecure code.

NEW QUESTION # 51
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 # 52
A company has been facing recurring issues with SQL injection vulnerabilities affecting the products, leading to significant disruptions for customers. To address the security concerns proactively, the company wants to integrate a tool into the CI/CD pipeline. The tool must be capable of identifying vulnerabilities such as SQL injection early in the development process, which allows developers to rectify issues before the code is deployed. Which solution must be implemented to meet the requirement?

- A. Dynamic Application Security Testing tools, such as OWASP ZAP, Veracode, Burp Suite
- B. workflow automation tools, such as GitHub Actions, Azure
- C. Static Application Security Testing tools, such as Checkmarx, Fortify, SonarQube
- D. build log observability tools, such as Splunk, Datadog

Answer: C

Explanation:
In the framework of theDesigning Cisco Security Infrastructure (300-745 SDSI)curriculum, the "Shift- Left" security strategy is fundamental to modern DevSecOps. To identify vulnerabilities like SQL injection at the earliest possible stage-specifically before the code is even compiled or deployed-Static Application Security Testing (SAST)is the required solution. SAST tools analyze the application's source code, byte code, or binaries without actually executing the program.
By integrating SAST tools like Checkmarx or SonarQube into the CI/CD pipeline, the security team can automate the scanning of every code commit or pull request. These tools use sophisticated algorithms to trace data flows and identify dangerous patterns, such as user-controlled input being concatenated directly into SQL queries without proper sanitization or parameterization. This proactive approach allows developers to receive immediate feedback within their native workflow, enabling them to fix security flaws before they progress into later, more expensive stages of the development lifecycle.
In contrast,Dynamic Application Security Testing (DAST)(Option D) requires a running instance of the application and typically occurs much later in the pipeline, such as during the testing or staging phase. While DAST is excellent for finding runtime vulnerabilities, it does not meet the requirement of identifying issues
"early in the development process" as effectively as SAST.Build log observability tools(Option B) and workflow automation platforms(Option C) provide infrastructure and visibility but do not possess the specialized engine required to perform deep code analysis for application-layer vulnerabilities like SQL injection. Implementing SAST ensures that security is a foundational element of the code-writing phase, aligning with Cisco's vision for a secure, automated software supply chain.

NEW QUESTION # 53
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. eBPF
- B. distributed firewall
- C. NGFW
- D. VPP

Answer: A

Explanation:
In modern secure infrastructure design, especially within high-performance testing and developer environments, the ability to observe and filter traffic at a deep level is crucial. eBPF (extended Berkeley Packet Filter) is a revolutionary technology that allows

developers to run sandboxed programs within the Linux kernel. The primary advantage of eBPF is that it enables sophisticated tracing, monitoring, and network filtering capabilities without the need to modify the underlying kernel source code or load intrusive kernel modules.
In the context of the Cisco SDSI objectives, eBPF is highlighted as a key component of distributed firewalling and cloud-native security architectures. It operates by attaching programs to various "hooks" in the kernel, such as network events, tracepoints, or system calls. When a packet enters the system or a specific event occurs, the eBPF program can inspect the context and make high-speed decisions on whether to allow, drop, or redirect traffic. This provides a much more efficient and flexible alternative to traditional technologies like IPTables. Because eBPF programs are verified for safety by a JIT compiler before being executed, they do not risk crashing the kernel, making them ideal for dynamic developer environments. Unlike Vector Packet Processing (VPP) (Option D), which moves packet processing into userspace, or standard Next-Generation Firewalls (NGFW) (Option C), which are typically separate appliances, eBPF provides "in-kernel" observability and enforcement that is programmable and highly scalable for microservices and containerized applications.

NEW QUESTION # 54
.....

If you want to pass the exam smoothly buying our Designing Cisco Security Infrastructure guide dump is your ideal choice. They can help you learn efficiently, save your time and energy and let you master the useful information. Our passing rate of 300-745 study tool is very high and you needn't worry that you have spent money and energy on them but you gain nothing. We provide the great service after you purchase our 300-745 cram training materials and you can contact our customer service at any time during one day. It is a pity if you don't buy our 300-745 study tool to prepare for the test Cisco certification.