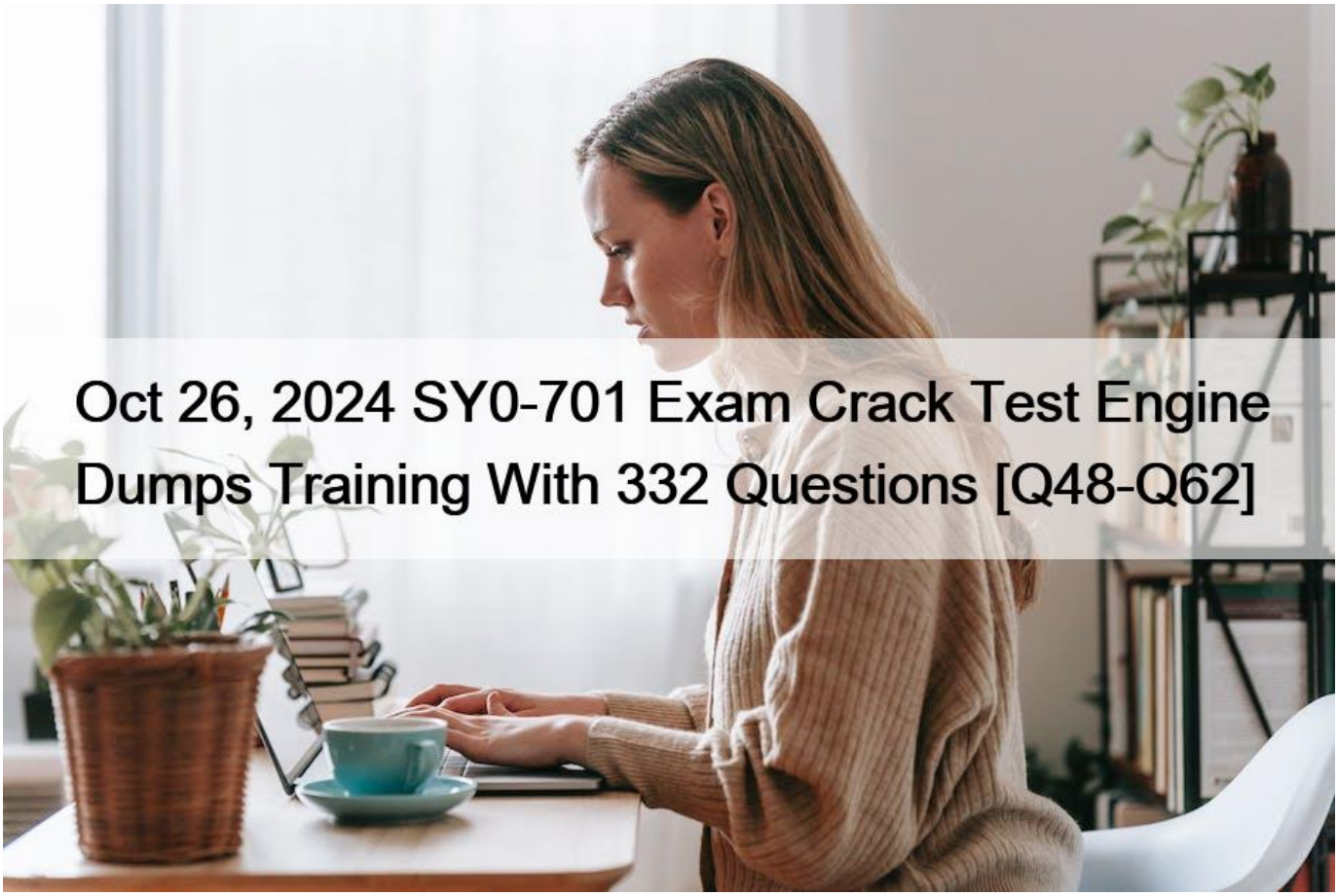
Oct 26, 2024 SY0-701 Exam Crack Test Engine Dumps Training With 332 Questions [Q48-Q62



Oct 26, 2024 SY0-701 Exam Crack Test Engine Dumps Training With 332 Questions Obtain the SY0-701 PDF Dumps Get 100% Outcomes Exam Questions For You To Pass Q48. Which of the following is the best reason to complete an audit in a banking environment?

* Regulatory requirement
* Organizational change
* Self-assessment requirement
* Service-level requirement

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization.

References:

Official CompTIA Security+ Study Guide (SY0-701), page 507

Security+ (Plus) Certification | CompTIA IT Certifications 2

Q49. Which of the following can be used to identify potential attacker activities without affecting production servers?
* Honey pot
* Video surveillance
* Zero Trust
* Geofencing

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker’s methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker’s attention from the real targets and waste their time and resources12.

The other options are not effective ways to identify potential attacker activities without affecting production servers:

* Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker’s activities on the network or the servers3.

* Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker’s activities on the network or the servers4.

* Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker’s activities on the network or the servers5.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception – SY0-601 CompTIA Security+ : 2.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985:

CompTIA Security+ SY0-701 Certification Study Guide, page 99.

Q50. An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?
* Virus
* Trojan
* Spyware
* Ransomware

Ransomware is a type of malware that encrypts the victim’s files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms.

Q51. Which of the following should a systems administrator set up to increase the resilience of an application by splitting the traffic between two identical sites?
* Load balancing
* Geographic disruption
* Failover
* Parallel processing

To increase the resilience of an application by splitting the traffic between two identical sites, a systems administrator should set up load balancing. Load balancing distributes network or application traffic across multiple servers or sites, ensuring no single server becomes overwhelmed and enhancing the availability and reliability of applications.

Load balancing: Distributes traffic across multiple servers to ensure high availability and reliability. It helps in managing the load efficiently and can prevent server overloads.

Geographic disruption: Not a standard term related to resilience. This might imply the use of geographically distributed sites but isn’t the precise solution described.

Failover: Refers to switching to a standby server or system when the primary one fails. It doesn’t inherently split traffic but rather takes over when a failure occurs.

Parallel processing: Refers to the simultaneous processing of tasks, not specifically related to load balancing web traffic.

Q52. The Chief Information Security Officer of an organization needs to ensure recovery from ransomware would likely occur within the organization’s agreed-upon RPOs end RTOs. Which of the following backup scenarios would best ensure recovery?
* Hourly differential backups stored on a local SAN array
* Dally full backups stored on premises in magnetic offline media
* Daly differential backups maintained by a third-party cloud provider
* Weekly full backups with daily incremental stored on a NAS drive

A backup strategy that combines weekly full backups with daily incremental backups stored on a NAS (Network Attached Storage) drive is likely to meet an organization’s Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). This approach ensures that recent data is regularly backed up and that recovery can be done efficiently, without significant data loss or lengthy downtime.

References =

* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

* CompTIA Security+ SY0-601 Study Guide: Chapter on Disaster Recovery and Backup Strategies.

Q53. An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?
* Deploying a SASE solution to remote employees
* Building a load-balanced VPN solution with redundant internet
* Purchasing a low-cost SD-WAN solution for VPN traffic
* Using a cloud provider to create additional VPN concentrators

SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions.

Q54. A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?
* Implementing a bastion host
* Deploying a perimeter network
* Installing a WAF
* Utilizing single sign-on

Q55. Which of the following would be the best way to handle a critical business application that is running on a legacy server?
* Segmentation
* Isolation
* Hardening
* Decommissioning

The device is STILL running a critical application. therefore it needs to be connected to the network. a compensating mechanism for this scenario would be segmentation as this would limit the ability of an attacker to pivot from the vulnerable server to the rest of the network.as possible.

Q56. A company is developing a critical system for the government and storing project information on a fileshare.

Which of the following describes how this data will most likely be classified? (Select two).
* Private
* Confidential
* Public
* Operational
* Urgent
* Restricted

Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:

Public: Data that can be freely disclosed to anyone without any harm or risk.

Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.

Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.

In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2. References: 1: CompTIA Security+ Study Guide: Exam SY0-701,

9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

Q57. Which of the following security control types does an acceptable use policybestrepresent?
* Detective
* Compensating
* Corrective
* Preventive

An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network1.

An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or

administrative in nature2.

Some examples of preventive controls are:

Locks, fences, or guards that prevent unauthorized physical access to a facility or a device Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:

Downloading or installing unauthorized or malicious software

Accessing or sharing sensitive or confidential information without authorization or encryption Using the network or the system for personal, illegal, or unethical purposes Bypassing or disabling security controls or mechanisms Connecting unsecured or unapproved devices to the network By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions3.

References = 1: How to Create an Acceptable Use Policy – CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy – CompTIA

Q58. Which of the following are common VoIP-associated vulnerabilities? (Choose two).
* SPIM
* Vishing
* VLAN hopping
* Phishing
* DHCP snooping
* Tailgating

SPIM (Spam over Internet Messaging) poses a threat to VoIP systems by consuming bandwidth, diverting resources, and potentially causing denial of service attacks. The influx of SPIM messages can degrade the quality of VoIP calls, overload servers, and serve as a platform for social engineering attacks, jeopardizing the security of VoIP users. To mitigate these risks, organizations should implement spam filters, intrusion detection systems, and regular software updates while also educating users to recognize and avoid potential threats associated with SPIM.

Q59. Which of the following would be the best way to block unknown programs from executing?
* Access control list
* Application allow list.
* Host-based firewall
* DLP solution

An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network12.

The other options are not the best ways to block unknown programs from executing:

Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object. An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing13.

Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing1 .

DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing1 .

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting – CompTIA Security+ SY0-701 – 3.5, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

Q60. A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.

Which of the following is the most important consideration during development?
* Scalability
* Availability
* Cost
* Ease of deployment

Explanation

Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of-service attacks, and have backup and recovery plans in case of failures2.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

Q61. A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?
* Packet captures
* Vulnerability scans
* Metadata
* Dashboard

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria.

A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors.

A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14. Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors.

Q62. Which of the following must be considered when designing a high-availability network? (Choose two).
* Ease of recovery
* Ability to patch
* Physical isolation
* Responsiveness
* Attack surface
* Extensible authentication

Explanation

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors12:

* Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.

* Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

* Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

* Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network,

* but it can also reduce the availability and accessibility of the network resources.

* Responsiveness: This refers to the speed and quality of the network’s performance and service delivery.

Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss.

Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

* Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor Messer.

SY0-701 Exam Dumps Contains FREE Real Quesions from the Actual Exam:
https://www.vceprep.com/SY0-701-latest-vce-prep.html]