SY0-701 Q&As

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations\\' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU

B. ISA

C. SLA

D. NDA

Correct Answer: A

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.

QUESTION 2

Development team members set up multiple application environments so they can develop, test, and deploy code in a secure and reliable manner. One of the environments is configured with real data that has been obfuscated so the team can adequately assess how the code will work in production. Which of the following environments is set up?

A. Quality assurance

B. Development

C. Sandbox

D. Production

Correct Answer: C

QUESTION 3

Which of the following involves an attempt to take advantage of database misconfigurations?

A. Buffer overflow

B. SQL injection

C. VM escape

D. Memory injection

Correct Answer: B

SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

QUESTION 4

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

A. Automation

B. Compliance checklist

C. Attestation

D. Manual audit

Correct Answer: A

Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise

require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs. Automation can be used to monitor, audit, and enforce

security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or

compromise12.

The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:

Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are

aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3. Attestation: This is a process of verifying or confirming the validity or

accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that

may occur on a daily basis4.

Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-

consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a

daily basis.

References: 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022:

Automation and Scripting -CompTIA Security+ SY0-701 -5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA

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

QUESTION 5

Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall

B. System isolation

C. Least privilege

D. Application allow list

Correct Answer: D

An application allow list is a security technique that specifies which applications are authorized to run on a system and blocks all other applications. An application allow list can best protect against an employee inadvertently installing malware on a company system because it prevents the execution of any unauthorized or malicious software, such as viruses, worms, trojans, ransomware, or spyware. An application allow list can also reduce the attack surface and improve the performance of the system.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 551 1

QUESTION 6

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

A. XDR

B. SPF

C. DLP

D. DMARC

Correct Answer: C

To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented. XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn\\'t specifically address data exfiltration. SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration. DMARC (Domain-based Message Authentication, Reporting and Conformance) also addresses email security and spoofing, not data exfiltration.

QUESTION 7

Which of the following tasks is typically included in the BIA process?

A. Estimating the recovery time of systems

B. Identifying the communication strategy

C. Evaluating the risk management plan

D. Establishing the backup and recovery procedures

E. Developing the incident response plan

Correct Answer: A

Estimating the recovery time of systems is a task typically included in the Business Impact Analysis (BIA) process. BIA involves identifying the critical functions of a business and determining the impact of a disruption. This includes estimating

how long it will take to recover systems and resume normal operations. Estimating the recovery time of systems: A key component of BIA, which helps in understanding the time needed to restore systems and services after a disruption.

Identifying the communication strategy: Typically part of the incident response plan, not BIA.

Evaluating the risk management plan: Part of risk management, not specifically BIA.

Establishing the backup and recovery procedures: Important for disaster recovery, not directly part of BIA.

Developing the incident response plan: Focuses on responding to security incidents, not on the impact analysis.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management process (Business Impact Analysis - BIA).

QUESTION 8

Which of the following security concepts is accomplished with the installation of a RADIUS server?

A. CIA

B. AAA

C. ACL

D. PEM

Correct Answer: B

The installation of a RADIUS server (Remote Authentication Dial-In User Service) is primarily associated with the security concept of AAA, which stands for Authentication, Authorization, and Accounting. RADIUS servers are used to manage

user credentials and permissions centrally, ensuring that only authenticated and authorized users can access network

resources, and tracking user activity for accounting purposes. Authentication: Verifies the identity of a user or device.

When a user tries to access a network, the RADIUS server checks their credentials (username and password) against a database.

Authorization: Determines what an authenticated user is allowed to do. After authentication, the RADIUS server grants permissions based on predefined policies. Accounting: Tracks the consumption of network resources by users. This

involves logging session details such as the duration of connections and the amount of data transferred.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.6 - Implement and maintain identity and access management.

QUESTION 9

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching

B. Data masking

C. Steganography

D. Salting

Correct Answer: D

Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks.

QUESTION 10

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

A. Whaling

B. Credential harvesting

C. Prepending

D. Dumpster diving

Correct Answer: D

Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could

involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of proper disposal and physical security

measures in cyber hygiene practices.

References:

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations. CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene.

QUESTION 11

Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

A. EOL

B. SLA

C. MOU

D. EOSL

Correct Answer: B

A document that provides expectations at a technical level for quality, availability, and responsibilities is a Service Level Agreement (SLA). An SLA is a contract between a service provider and a customer that specifies the level of service that the provider will deliver. This typically includes technical details such as uptime, response times, and performance criteria. The SLA is used to ensure that the customer receives the level of service that they have agreed to and that the provider is held accountable for meeting those expectations. Options A, C, and D are not related to the technical level of service expectations. EOL refers to the end of life for a product or service, MOU is a memorandum of understanding, and EOSL is the end of service life.

QUESTION 12

A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

A. Serverless architecture

B. Thin clients

C. Private cloud

D. Virtual machines

Correct Answer: A

Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing

code, while the cloud provider manages the servers, scaling, and maintenance. Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.

References:

CompTIA Security+ SY0-701 Course Content: The course covers cloud technologies, including serverless architectures, which are highlighted as a method to streamline and reduce costs associated with code deployment.

QUESTION 13

Which of the following can a security director use to prioritize vulnerability patching within a company\\'s IT environment?

A. SOAR

B. CVSS

C. SIEM

D. CVE

Correct Answer: B

The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of security vulnerabilities. It helps organizations prioritize vulnerability patching by providing a numerical score that reflects the

potential impact and exploitability of a vulnerability. CVSS scores are used to gauge the urgency of patching vulnerabilities within a company\\'s IT environment.

References:

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

CompTIA Security+ SY0-601 Study Guide: Chapter on Vulnerability Management.

QUESTION 14

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

A. Tuning

B. Aggregating

C. Quarantining

D. Archiving

Correct Answer: A

Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is

also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options.

References: Security Alerting and Monitoring Concepts and Tools -CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

QUESTION 15

An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?

A. Partially known environment

B. Unknown environment

C. Integrated

D. Known environment

Correct Answer: A

A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test1.

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.