SY0-701$^{\text{Q\&As}}$

CompTIA Security+

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

A. Deploying PowerShell scripts

B. Pushing GPO update

C. Enabling PAP

D. Updating EDR profiles

Correct Answer: B

A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password

policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment. References:

CompTIA Security+ Study Guide:

Exam SY0-701, 9th Edition, page 115; Password Policy - Windows Security

QUESTION 2

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

A. Air gap the system.

B. Move the system to a different network segment.

C. Create a change control request.

D. Apply the patch to the system.

Correct Answer: C

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches.

References: CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

QUESTION 3

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A. Hardening

B. Employee monitoring

C. Configuration enforcement

D. Least privilege

Correct Answer: D

The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data

and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices. However, it is rarely implemented in practice. In this

scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users:

the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to

the normal user interface of the software, which is sufficient for them to perform their job functions. The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing

unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers\\' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration

enforcement is the process of ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a policy, or a template.

References:

https://en.wikipedia.org/wiki/Principle_of_least_privilege https://en.wikipedia.org/wiki/Principle_of_least_privilege

QUESTION 4

Which of the following security controls is used to isolate a section of the network and its externally available resources from the internal corporate network in order to reduce the number of possible attacks?

A. Faraday cages

B. Air gap

C. Vaulting

D. Proximity readers

Correct Answer: B

QUESTION 5

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee\\'s corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

A. Application

B. IPS/IDS

C. Network

D. Endpoint

Correct Answer: D

An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable. An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown. An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols. A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers. Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.

References: https://www.crowdstrike.com/cybersecurity-101/observability/application-log/ https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

QUESTION 6

A business received a small grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?

A. Security of cloud providers

B. Cost of implementation

C. Ability of engineers

D. Security of architecture

Correct Answer: D

Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud infrastructure.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 3491

QUESTION 7

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

A. Off-the-shelf software

B. Orchestration

C. Baseline

D. Policy enforcement

Correct Answer: B

Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457 1

QUESTION 8

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I\\'m in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.

B. Add a smishing exercise to the annual company training.

C. Issue a general email warning to the company.

D. Have the CEO change phone numbers.

E. Conduct a forensic investigation on the CEO\\'s phone.

F. Implement mobile device management.

Correct Answer: BC

This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money.

References: What Is Phishing | Cybersecurity | CompTIA, Phishing -SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

QUESTION 9

During a penetration test, a vendor attempts to enter an unauthorized area using an access badge. Which of the following types of tests does this represent?

A. Defensive

B. Passive

C. Offensive

D. Physical

Correct Answer: D

QUESTION 10

An organization\\'s internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW

B. WAF

C. TLS

D. SD-WAN

Correct Answer: B

A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization\\'s internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data.

References: Buffer Overflows -CompTIA Security+ SY0-701 ?2.3, Web Application Firewalls -CompTIA Security+ SY0-701 ?2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

QUESTION 11

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 12

After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

A. CASB

B. VPC

C. SWG

D. CMS

Correct Answer: A

CASB vs SWG CASB is the more optimal solution for multiple on premises security solutions CASB services are explicitly designed to fit the needs of large enterprises You can access link and read about it:

https://www.gend.co/blog/casb-or-swg-which-is-best-option-for-your-enterprise

QUESTION 13

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A. RDP server

B. Jump server

C. Proxy server

D. Hypervisor

Correct Answer: B

A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the

jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can

also enforce security policies, such as authentication, authorization, logging, and auditing, on the user\\'s connection. A jump server is also known as a bastion host or a jump box.

References:

CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other

Network Appliances -SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question2.

QUESTION 14

A software developer would like to ensure the source code cannot be reverse engineered or debugged. Which of the following should the developer consider?

A. Version control

B. Obfuscation toolkit

C. Code reuse

D. Continuous integration

E. Stored procedures

Correct Answer: B

An obfuscation toolkit is used by developers to make source code difficult to understand and reverse engineer. This technique involves altering the code\\'s structure and naming conventions without changing its functionality, making it much

harder for attackers to decipher the code or use debugging tools to analyze it. Obfuscation is an important practice in protecting proprietary software and intellectual property from reverse engineering.

References:

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture. CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Coding Practices.

QUESTION 15

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

A. Accept

B. Transfer

C. Mitigate

D. Avoid

Correct Answer: B

Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of- service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are: Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high. Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk. Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable. Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high. By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B. Transfer.

References: CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer\\'s CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).