Free Questions for SY0-701 by certsinside

Shared by Davis on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Security of cloud providers

B- Cost of implementation

C- Ability of engineers

D- Security of architecture

Answer:

D

Explanation:

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

Question 2

Question Type: MultipleChoice

A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

Options:

A- Host-based firewall

B- Web application firewall

C- Access control list

D- Application allow list

Answer:

A

Explanation:

A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers.A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

Question 3

Question Type: MultipleChoice

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

Options:

A- IDS

B- ACL

C- EDR

D- NAC

Answer:

C

Explanation:

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources.EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance

status.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

Question 4

Question Type: MultipleChoice

A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

Options:

A- Attribute-based

B- Time of day

C- Role-based

D- Least privilege

Answer:

D

Explanation:

The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer.Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

Question 5

Question Type: MultipleChoice

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

Options:

A- Insider threat

B- Email phishing

C- Social engineering

D- Executive whaling

Answer:

C

Explanation:

Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk.The other topics are not relevant to this situation.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 191

Question 6

Question Type: MultipleChoice

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

Options:

A- Configure all systems to log scheduled tasks.

B- Collect and monitor all traffic exiting the network.

C- Block traffic based on known malicious signatures.

D- Install endpoint management software on all systems.

Answer:

D

Explanation:

Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints.The other options are not as effective or comprehensive as endpoint management software for this purpose.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1371

Question 7

Question Type: MultipleChoice

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

Options:

A- Impact analysis

B- Scheduled downtime

C- Backout plan

D- Change management boards

Answer:

B

Explanation:

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the

normal business operations or affecting the availability of the system or service.Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 5791

Question 8

Question Type: MultipleChoice

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

Options:

A- EAP

B- DHCP

C- IPSec

D- NAT

Answer:

C

Explanation:

IPSec is a protocol suite that provides secure communication over IP networks. IPSec can be used to create virtual private networks (VPNs) that encrypt and authenticate the data exchanged between two or more parties. IPSec can also provide data integrity, confidentiality, replay protection, and access control.A security consultant can use IPSec to gain secure, remote access to a client environment by establishing a VPN tunnel with the client's network.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 3851

Question 9

Question Type: MultipleChoice

After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP

Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test:

nmap -p 23 192.168.14.6 ---script telnet-encryption

PORT STATE SERVICE REASON

23/tcp open telnet syn-ack

I telnet encryption:

| _ Telnet server supports encryption

Which of the following would the security analyst conclude for this reported vulnerability?

Options:

A- It is a false positive.

B- A rescan is required.

C- It is considered noise.

D- Compensating controls exist.

Answer:

A

Explanation:

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server.The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly3. Reference:3:Telnet Protocol - Can You Encrypt Telnet?

Question 10

Question Type: MultipleChoice

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).

Options:

A- Private

B- Confidential

C- Public

D- Operational

E- Urgent

F- Restricted

Answer:

B, F

Explanation:

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. Reference:1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-172:Data Classification Practices: Final Project Description Released

Question 11

Question Type: MultipleChoice

A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

Options:

A- Patch availability

B- Product software compatibility

C- Ease of recovery

D- Cost of replacement

Answer:

A

Explanation:

End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues.Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 291

Question 12

Question Type: MultipleChoice

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

Options:

A- Insider threat

B- Hacktivist

C- Nation-state

D- Organized crime

Answer:

D

Explanation:

Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit.Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 171