Free Questions for Cybersecurity-Audit-Certificate by certsinside

Shared by Holloway on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What should be an IS auditor's GREATEST concern when an organization's virtual private network (VPN) is implemented on employees' personal mobile devices?

Options:

A- Users may access services over the VPN that are network resource intensive.

B- Users may store the data in plain text on their mobile devices.

C- Users may access the corporate network from unauthorized devices.

D- Users may access services not supported by the VPN.

Answer:

B

Explanation:

When employees use personal mobile devices to access a VPN, the greatest concern for an IS auditor is the potential for sensitive data to be stored in an unsecured manner. If data is stored in plain text, it could be easily accessed by unauthorized parties if the device is lost, stolen, or compromised. This risk is heightened when the devices are not managed by the organization's IT department, which would typically enforce security policies such as encryption.

Question 2

Question Type: MultipleChoice

Which of the following describes a system that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet?

Options:

A- Intrusion detection system (IDS)

B- Intrusion prevention system (IPS)

C- Firewall

D- Router

Answer:

C

Explanation:

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It establishes a barrier between a secure internal network and an untrusted external network, such as the internet. This system is designed to prevent unauthorized access to or from private networks and is a fundamental piece of a comprehensive security framework for any organization.

Question 3

Question Type: MultipleChoice

Which type of firewall blocks many types of attacks, such as cross-site scripting (XSS) and structured query language (SQL) injection?

Options:

A- Intrusion detection

B- Stateful inspection

C- Host-based

D- Web application

Answer:

D

Explanation:

A web application firewall (WAF) is specifically designed to monitor, filter, and block HTTP traffic to and from a web application. It is different from other types of firewalls because it can filter the content of specific web applications. By inspecting HTTP traffic, a WAF can prevent attacks stemming from web application security flaws, such as SQL injection and cross-site scripting (XSS), file inclusion, and security misconfigurations.

Question 4

Question Type: MultipleChoice

Which of the following is a team created PRIMARILY to improve the security posture of an organization?

Options:

A- Computer emergency response team (CERT)

B- Security operations center (SOC) team

C- Disaster recovery team

D- Risk management team

Answer:

B

Explanation:

The primary purpose of a Security Operations Center (SOC) team is to continuously monitor and improve an organization's security posture. They are responsible for the detection, analysis, and response to cybersecurity incidents, using a combination of technology solutions and a strong set of processes.

Reference= ISACA's resources highlight the role of SOC teams in enhancing the security measures of an organization.They are integral to the proactive defense against cyber threats and play a key role in the strategic planning of security measures123.

Question 5

Question Type: MultipleChoice

Which of the following is a known potential risk of using a software defined perimeter (SDP) controller?

Options:

A- Unauthorized access may jeopardize data confidentiality, integrity, or availability.

B- Operations may be adversely affected if data cannot be recovered and restored timely.

C- Unauthorized use of valid credentials may compromise encrypted data at rest.

D- An ineffective firewall may fail to identify and block unwanted network traffic.

Answer:

A

Explanation:

One of the known potential risks of using a Software Defined Perimeter (SDP) controller is unauthorized access, which can jeopardize the confidentiality, integrity, or availability of data. SDP controllers work by creating a boundary around network resources, but if an unauthorized user gains access, perhaps through stolen credentials or exploitation of a vulnerability, they could potentially access sensitive data or disrupt services.

Question 6

Question Type: MultipleChoice

Which of the following describes computing capabilities that are available over the network and can be accessed by diverse client platforms?

Options:

A- Resource pooling

B- Shared network access

C- Private network access

D- Broad network access

Answer:

D

Explanation:

Broad network access refers to the computing capabilities that are available over a network and can be accessed by diverse client platforms, such as personal computers, mobile phones, and tablets. This characteristic is one of the essential features of cloud computing, which allows users to access services using a variety of devices through standard mechanisms.

Question 7

Question Type: MultipleChoice

In the context of network communications, what are the two types of attack vectors?

Options:

A- Ingress and egress

B- Physical theft and loss

C- Insider and privilege misuse

D- Malware and phishing

Answer:

A

Explanation:

In the context of network communications, the two types of attack vectors are ingress and egress. Ingress refers to the unauthorized entry or access to a network, which can include various forms of cyberattacks aimed at penetrating network defenses.Egress, on the other hand, involves the unauthorized transmission of data out of a network, often as part of data exfiltration efforts by attackers1.

Question 8

Question Type: MultipleChoice

Which of the following provides additional protection other than encryption to messages transmitted using portable wireless devices?

Options:

A- Endpoint protection

B- Intrusion detection system (IDS)

C- Virtual private network (VPN)

D- Intrusion prevention system (IPS)

Answer:

C

Explanation:

A Virtual Private Network (VPN) provides additional protection to messages transmitted using portable wireless devices by creating a secure and encrypted tunnel for data transmission. This helps protect the data from being intercepted or accessed by unauthorized entities. While encryption secures the content of the messages, a VPN secures the transmission path, adding an extra layer of security.

Question 9

Question Type: **MultipleChoice**

Which of the following is an important reason for tracing the access and origin of an intrusion once it has been detected?

Options:

A- To create appropriate security awareness content to avoid recurrence

B- To determine the impact of the intrusion event

C- To perform a root cause analysis of the intrusion event

D- To determine and correct any system weaknesses

Answer:

C

Explanation:

Tracing the access and origin of an intrusion is crucial for performing a root cause analysis. This process involves identifying the underlying factors that led to the security breach. By understanding how the intrusion happened, organizations can better address the specific vulnerabilities that were exploited and implement more effective security measures to prevent similar incidents in the future.

Question 10

Question Type: MultipleChoice

Which of the following is the MAIN reason why domain name system (DNS) data exfiltration is a significant threat to mobile computing?

Options:

A- It is simple to inject malformed code to compromise data processing.

B- It is easy to execute command and control of the mobile target.

C- It is difficult to distinguish malicious activity from legitimate traffic.

D- There is relative anonymity of network connections outside the organization.

Answer:

C

Explanation:

DNS data exfiltration poses a significant threat to mobile computing mainly because it is challenging to differentiate between malicious activity and legitimate DNS traffic. Attackers can exploit this by embedding data within DNS queries and responses, which often go unnoticed because DNS traffic is generally allowed through firewalls and security systems without triggering alerts. This method of data theft can be particularly effective in mobile computing, where devices frequently switch networks and rely on DNS for connectivity.

Reference= ISACA's resources on cybersecurity risks associated with DNS highlight the difficulty in detecting DNS data exfiltration due to its ability to blend in with normal traffic.This is further supported by industry resources that discuss the challenges in identifying and preventing such exfiltration techniques1234.