KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CCOA**

Title : ISACA Certified Cybersecurity Operations Analyst

Version : DEMO

1.Which of the following is a PRIMARY risk that can be introduced through the use of a site-to-site virtual private network (VPN) with a service provider?
A. Loss of data integrity
B. Gaps in visibility to user behavior
C. Data exfiltration
D. Denial of service (DoS) attacks
Answer: B
Explanation:
Site-to-site VPNs establish secure, encrypted connections between two networks over the internet, typically used to link corporate networks with remote sites or a service provider's network. However, while these VPNs secure data transmission, they introduce specific risks.
The primary risk associated with a site-to-site VPN with a service provider is the loss of visibility into user behavior. Here’s why:
Limited Monitoring: Since the traffic is encrypted and routed through the VPN tunnel, the organization may lose visibility over user activities within the service provider's network.
Blind Spots in Traffic Analysis: Security monitoring tools (like IDS/IPS) that rely on inspecting unencrypted data may be ineffective once data enters the VPN tunnel.
User Behavior Analytics (UBA) Issues: It becomes challenging to track insider threats or compromised accounts due to the encapsulation and encryption of network traffic.
Vendor Dependency: The organization might depend on the service provider’s security measures to detect malicious activity, which may not align with the organization’s security standards.
Other options analysis:
A. Loss of data integrity: VPNs generally ensure data integrity using protocols like IPsec, which validates packet integrity.
C. Data exfiltration: While data exfiltration can occur, it is typically a consequence of compromised credentials or insider threats, not a direct result of VPN usage.
D. Denial of service (DoS) attacks: While VPN endpoints can be targeted in a DoS attack, it is not the primary risk specific to VPN use with a service provider.
CCOA Official Review Manual, 1st Edition
Reference: Chapter 4: Network Security Operations: Discusses risks related to VPNs, including reduced visibility.
Chapter 7: Security Monitoring and Incident Detection: Highlights the importance of maintaining visibility even when using encrypted connections.
Chapter 8: Incident Response and Recovery: Addresses challenges related to VPN monitoring during incidents.

2.A bank employee is found to be exfiltration sensitive information by uploading it via email.
Which of the following security measures would be MOST effective in detecting this type of insider threat?
A. Data loss prevention (DIP)
B. Intrusion detection system (IDS)
C. Network segmentation
D. Security information and event management (SIEM)
Answer: A

Explanation:
Data Loss Prevention (DLP) systems are specifically designed to detect and prevent unauthorized data transfers. In the context of an insider threat, where a bank employee attempts to exfiltrate sensitive information via email, DLP solutions are most effective because they:
Monitor Data in Motion: DLP can inspect outgoing emails for sensitive content based on pre-defined rules and policies.
Content Inspection and Filtering: It examines email attachments and the body of the message for patterns that match sensitive data (like financial records or PII).
Real-Time Alerts: Generates alerts or blocks the transfer when sensitive data is detected.
Granular Policies: Allows customization to restrict specific types of data transfers, including via email.
Other options analysis:
B. Intrusion detection system (IDS): IDS monitors network traffic for signs of compromise but is not designed to inspect email content or detect data exfiltration specifically.
C. Network segmentation: Reduces the risk of lateral movement but does not directly monitor or prevent data exfiltration through email.
D. Security information and event management (SIEM): SIEM can correlate events and detect anomalies but lacks the real-time data inspection that DLP offers.
CCOA Official Review Manual, 1st Edition
Reference: Chapter 5: Insider Threats and Mitigation: Discusses how DLP tools are essential for detecting data
exfiltration.
Chapter 6: Threat Intelligence and Analysis: Covers data loss scenarios and the role of DLP.
Chapter 8: Incident Detection and Response: Explains the use of DLP for detecting insider threats.

3.Which of the following network topologies is MOST resilient to network failures and can prevent a single point of failure?
A. Mesh
B. Star
C. Bus
D. Ring
Answer: A
Explanation:
A mesh network topology is the most resilient to network failures because:
Redundancy: Each node is interconnected, providing multiple pathways for data to travel.
No Single Point of Failure: If one connection fails, data can still be routed through alternative paths.
High Fault Tolerance: The decentralized structure ensures that the failure of a single device or link does not significantly impact network performance.
Ideal for Critical Infrastructure: Often used in environments where uptime is critical, such as financial or emergency services networks.
Other options analysis:
B. Star: A central hub connects all nodes, so if the hub fails, the entire network collapses.
C. Bus: A single backbone cable means a break in the cable can disrupt the entire network.
D. Ring: Data travels in a circular path; a single break can isolate part of the network unless it is a dual-ring topology.

CCOA Official Review Manual, 1st Edition
Reference: Chapter 4: Network Security Operations: Discusses network topology and its impact on reliability and redundancy.
Chapter 9: Network Design and Architecture: Highlights resilient topologies, including mesh, for secure and fault-tolerant operations.

4.Which of the following is MOST likely to result from a poorly enforced bring your own device (8YOD) policy?
A. Weak passwords
B. Network congestion
C. Shadow IT
D. Unapproved social media posts
Answer: C
Explanation:
A poorly enforced Bring Your Own Device (BYOD) policy can lead to the rise of Shadow IT, where employees use unauthorized devices, software, or cloud services without IT department approval. This often occurs because:
Lack of Policy Clarity: Employees may not be aware of which devices or applications are approved.
Absence of Monitoring: If the organization does not track personal device usage, employees may introduce unvetted apps or tools.
Security Gaps: Personal devices may not meet corporate security standards, leading to data leaks and vulnerabilities.
Data Governance Issues: IT departments lose control over data accessed or stored on unauthorized devices, increasing the risk of data loss or exposure.
Other options analysis:
A. Weak passwords: While BYOD policies might influence password practices, weak passwords are not directly caused by poor BYOD enforcement.
B. Network congestion: Increased device usage might cause congestion, but this is more of a performance issue than a security risk.
D. Unapproved social media posts: While possible, this issue is less directly related to poor BYOD policy enforcement.
CCOA Official Review Manual, 1st Edition
Reference: Chapter 3: Asset and Device Management: Discusses risks associated with poorly managed BYOD policies.
Chapter 7: Threat Monitoring and Detection: Highlights how Shadow IT can hinder threat detection.

5.Which of the following roles typically performs routine vulnerability scans?
A. Incident response manager
B. Information security manager
C. IT auditor
D. IT security specialist
Answer: D
Explanation:
An IT security specialist is responsible for performing routine vulnerability scans as part of maintaining

the organization's security posture.
Their primary tasks include:
Vulnerability Assessment: Using automated tools to detect security flaws in networks, applications, and systems.
Regular Scanning: Running scheduled scans to identify new vulnerabilities introduced through updates or configuration changes.
Reporting: Analyzing scan results and providing reports to management and security teams.
Remediation Support: Working with IT staff to patch or mitigate identified vulnerabilities.
Other options analysis:
A. Incident response manager: Primarily focuses on responding to security incidents, not performing routine scans.
B. Information security manager: Manages the overall security program but does not typically conduct scans.
C. IT auditor: Reviews the effectiveness of security controls but does not directly perform scanning.
CCOA Official Review Manual, 1st Edition
Reference: Chapter 6: Vulnerability and Patch Management: Outlines the responsibilities of IT security specialists in conducting vulnerability assessments.
Chapter 8: Threat and Vulnerability Assessment: Discusses the role of specialists in maintaining security baselines.