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 : **312-39**

Title : Certified SOC Analyst (CSA)

Version : DEMO

1.The SOC team is tasked with enhancing the security of an organization's network infrastructure. The organization's public-facing web servers, which handle customer transactions, need to be isolated from the internal private network containing sensitive employee data and proprietary systems. The goal is to create a buffer zone that limits exposure of internal systems if the web servers are compromised during a cyberattack, such as a DDoS or SQL injection attempt.
As a SOC analyst, which network architecture component would you recommend implementing to establish this isolated region?
A. Demilitarized Zone (DMZ)
B. Intrusion Detection System (IDS)
C. Firewall
D. Honeypot
Answer: A
Explanation:
A DMZ is the standard architecture component used to place internet-facing services (web, mail relays, reverse proxies) into a separate, controlled network segment that sits between the untrusted internet and the trusted internal network. From a SOC perspective, the DMZ reduces the impact of compromise by limiting lateral movement opportunities. Even if a web server is exploited (SQL injection, remote code execution, credential theft), the attacker is confined to a segment with strict, minimal access rules into internal systems. This is achieved by enforcing tightly scoped inbound and outbound traffic policies at the DMZ boundaries, typically allowing only necessary ports and explicitly approved flows (for example, web tier to app tier on a specific port, with no direct route to employee data networks). A firewall is a control that enforces policy, but the “isolated region/buffer zone” concept is specifically the DMZ. IDS and honeypots are detection/deception controls; they do not provide the segmentation boundary required to isolate public-facing systems from sensitive internal networks.

2.A Security Operations Center (SOC) analyst receives a high-priority alert indicating unusual user activity. An employee account is attempting to access company resources from a different country and outside of their normal working hours. This behavior raises concerns about potential account compromise or unauthorized access.
To automate the initial response and quickly restrict access while further investigating the incident, which SOAR playbook would be relevant to adapt and implement?
A. Alert Enrichment SOAR Playbook
B. Deprovisioning Users SOAR Playbook
C. Malware Containment SOAR Playbook
D. Phishing Investigations SOAR Playbook
Answer: B
Explanation:
When there is a strong indication of account compromise (impossible travel, unusual geography, out-of-hours access to sensitive resources), the priority is to reduce attacker dwell time by immediately restricting the account’s ability to authenticate and access data. A “Deprovisioning Users” playbook aligns best with this objective because it is focused on access removal actions such as disabling the user, revoking active sessions, resetting credentials, invalidating refresh tokens, removing risky group memberships, and blocking sign-in until verification is complete. Alert enrichment is valuable, but it does not stop the threat; it only adds context. Malware containment is oriented toward endpoint isolation and

malicious file/process containment, not identity-based risk. Phishing investigations is appropriate when the primary entry vector is suspected phishing and the goal is to analyze messages, URLs, and affected recipients, but it still may not provide the immediate identity lockdown needed. In SOC operations, identity compromise often demands rapid containment through account restriction first, followed by investigation to confirm legitimacy, determine scope, and safely restore access with stronger controls such as MFA and conditional access.

3.A leading e-commerce company relies on backend servers for processing customer transactions. You are working with their cybersecurity team as a SOC analyst. One morning, you notice a sharp increase in CPU utilization on one of your backend servers. Your team scans and monitors the server and finds that an unknown process is running, consuming excessive resources. You further perform detailed forensic analysis and identify the presence of an unrecognized scheduled task that triggers a PowerShell script connecting to an unknown IP address.
What should you do to confirm whether this is an active attack?
A. Analyze the network logs to identify external connections
B. Check file integrity and detect recent unauthorized changes
C. Analyze the system logs for unauthorized changes
D. Review user access logs for unauthorized activity
Answer: A
Explanation:
The strongest “must-be-true” confirmation for an active attack in this scenario is evidence of command-and-control (C2) or other suspicious external communication. You already have a scheduled task launching PowerShell and attempting to connect to an unknown IP address, which is a high-signal indicator of malicious automation. The fastest way to validate ongoing activity is to analyze network telemetry (firewall/proxy logs, netflow, EDR network events) to confirm whether outbound connections are occurring, how frequently, and whether data is being transferred. Network logs can reveal destination IP/port, protocols, connection success/failure, volume, and timing correlation with the scheduled task triggers. File integrity checks and system logs are useful for understanding persistence and modifications, but they may lag behind or miss short-lived network beacons. User access logs help attribute activity but do not directly confirm an active external control channel. From a SOC triage and containment perspective, confirming external connections enables immediate actions such as blocking the destination, isolating the host, and scoping for other systems contacting the same IPs/domains. Therefore, network log analysis is the most direct next step to confirm active malicious behavior.

4.One week after a ransomware attack disrupted operations, Sarah, a SOC analyst, leads a review meeting with the IT team, security engineers, and business unit representatives. The group reviews the incident timeline, calculates a business impact of $157,000 due to downtime and data loss, and identifies seven critical improvements to enhance detection and response processes.
Which of the following Incident Response phase is this?
A. Recovery
B. Post-Incident Activities
C. Eradication
D. Containment
Answer: B

Explanation:
This is the “Post-Incident Activities” phase, commonly known as lessons learned or post-incident review. The defining elements are present: the incident is already over (one week later), stakeholders are reviewing the timeline, calculating business impact, and identifying improvements to processes and controls. In SOC practice, this phase focuses on improving readiness and reducing recurrence by documenting what happened, what worked, what failed, and what should change. Typical outputs include updated playbooks/runbooks, improved detection logic, better alert triage workflows, logging and telemetry enhancements, refined escalation paths, improved backup/restore procedures, and training actions. Recovery is about restoring services and operations (rebuild systems, restore data, validate return-to-service), which is not the primary activity described. Eradication is removing the threat from the environment (remove malware, close persistence, patch exploited vulnerabilities). Containment is stopping spread and limiting damage during the incident. Since the group is assessing impact and creating improvement actions after operations have resumed, the correct classification is Post-Incident Activities.

5.An organization with a complex IT infrastructure is planning to implement a SIEM solution to improve its threat detection and response capabilities. Due to the scale and complexity of its systems, the organization opts for a phased deployment approach to ensure a smooth implementation and reduce potential risks.
Which of the following should be the first phase in their SIEM deployment strategy?
A. Automate incident response processes
B. Implement User and Entity Behavior Analytics (UEBA)
C. Set up the log management component before deploying the SIEM component
D. Configure security analytics to identify potential threats
Answer: C
Explanation:
The first phase should establish reliable log ingestion and storage—log management—before attempting advanced detection content or automation. A SIEM is only as effective as the data it receives. In a complex environment, initial success depends on building a stable pipeline: collecting logs from priority sources, normalizing timestamps, ensuring consistent parsing, defining retention, and validating data quality (completeness, latency, duplication, and integrity). Without this foundation, analytics will produce blind spots, false positives, and missed detections, and automation may take disruptive actions based on incomplete data. UEBA and security analytics are valuable but require sufficient historical, high-quality telemetry to build baselines and correlations. Similarly, incident response automation should come after the organization has validated detections, tuning, and operational workflows; otherwise, playbooks may amplify errors at scale. A phased approach typically starts with identifying key data sources (identity, endpoint, network, cloud), onboarding them into log management, confirming visibility and schema consistency, and only then layering detection rules, correlations, and response workflows. Therefore, setting up log management first is the correct starting phase for a low-risk, high-success SIEM deployment.