Free Questions for CS0-003 by ebraindumps

Shared by Armstrong on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following will most likely cause severe issues with authentication and logging?

Options:

A- Virtualization

B- Multifactor authentication

C- Federation

D- Time synchronization

Answer:

D

Explanation:

Time synchronization issues can cause severe problems with authentication and logging. If system clocks are not properly synchronized, it can lead to discrepancies in log timestamps, making it difficult to correlate events across different systems. Additionally, time-related discrepancies can affect authentication mechanisms that rely on time-based tokens, such as those used in multifactor authentication,

leading to failures and security gaps.

Question 2

Question Type: MultipleChoice

An organization has a critical financial application hosted online that does not allow event logging to send to the corporate SIEM. Which of the following is the best option for the security analyst to configure to improve the efficiency of security operations?

Options:

A- Configure a new SIEM specific to the management of the hosted environment.

B- Subscribe to a threat feed related to the vendor's application.

C- Use a vendor-provided API to automate pulling the logs in real time.

D- Download and manually import the logs outside of business hours.

Answer:

C

Question 3

Question Type: MultipleChoice

A development team is preparing to roll out a beta version of a web application and wants to quickly test for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. Which of the following tools would the security team most likely recommend to perform this test?

Options:

A- Has heat

B- OpenVAS

C- OWASP ZAP

D- Nmap

Answer:

C

Explanation:

OWASP ZAP (Zed Attack Proxy) is a tool recommended for quickly testing web applications for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. It is an open-source web application security scanner that helps identify security issues in web applications during the development and testing phases.

Question 4

Question Type: MultipleChoice

A cybersecurity analyst has been assigned to the threat-hunting team to create a dynamic detection strategy based on behavioral analysis and attack patterns. Which of the following best describes what the analyst will be creating?

Options:

A- Bots

B- loCs

C- TTPs

D- Signatures

Answer:

C

Explanation:

The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

Question 5

Question Type: MultipleChoice

Results of a SOC customer service evaluation indicate high levels of dissatisfaction with the inconsistent services provided after regular work hours. To address this, the SOC lead drafts a document establishing customer expectations regarding the SOC's performance and quality of services. Which of the following documents most likely fits this description?

Options:

A- Risk management plan

B- Vendor agreement

C- Incident response plan

D- Service-level agreement

Answer:

D

Explanation:

A Service-Level Agreement (SLA) is a document that establishes customer expectations regarding the performance and quality of services provided by the SOC (Security Operations Center). It defines the level of service expected, including aspects like response times, availability, and support after regular work hours. An SLA helps in setting clear expectations and improving customer satisfaction by outlining the standards and commitments of the service provider.

Question 6

Question Type: MultipleChoice

An MSSP received several alerts from customer 1, which caused a missed incident response deadline for customer 2. Which of the following best describes the document that was violated?

Options:

A- KPI

B- SLO

C- SLA

D- MOU

Answer:

C

Explanation:

The document that was violated in this scenario is the SLA (Service Level Agreement). An SLA is a formal agreement between a service provider and a customer that defines the level of service expected. It includes specific metrics such as response times and resolution times. Missing an incident response deadline for customer 2 due to alerts from customer 1 indicates a breach of the agreed-upon service levels outlined in the SLA.

Question 7

Question Type: **MultipleChoice**

An analyst investigated a website and produced the following:

Starting Nmap 7.92 (https://nmap.org) at 2022-07-21 10:21 CDT

Nmap scan report for insecure.org (45.33.49.119)

Host is up (0.054s latency).

rDNS record for 45.33.49.119: ack.nmap.org

Not shown: 95 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

25/tcp closed smtp

80/tcp open http Apache httpd 2.4.6

113/tcp closed ident

443/tcp open ssl/http Apache httpd 2.4.6

Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap .org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds

Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

Options:

A- nmap -sS -T4 -F insecure.org

B- nmap -0 insecure.org

C- nmap -sV -T4 -F insecure.org

D- nmap -A insecure.org

Answer:

C

Question 8

Question Type: **MultipleChoice**

During a tabletop exercise, engineers discovered that an ICS could not be updated due to hardware versioning incompatibility. Which of the following is the most likely cause of this issue?

Options:

A- Legacy system

B- Business process interruption

C- Degrading functionality

D- Configuration management

Answer:

A

Explanation:

The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

Question 9

Question Type: MultipleChoice

Which of the following best describes the key goal of the containment stage of an incident response process?

Options:

A- To limit further damage from occurring

B- To get services back up and running

C- To communicate goals and objectives of the incident response plan

D- To prevent data follow-on actions by adversary exfiltration

Answer:

A

Explanation:

The key goal of the containment stage in an incident response process is to limit further damage from occurring. This involves taking immediate steps to isolate the affected systems or network segments to prevent the spread of the incident and mitigate its impact. Containment strategies can be short-term, to quickly stop the incident, or long-term, to prepare for the eradication and recovery phases.

Question 10

Question Type: MultipleChoice

Several reports with sensitive information are being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

Options:

A- Implement step-up authentication for administrators.

B- Improve employee training and awareness.

C- Increase password complexity standards.

D- Deploy mobile device management.

Answer:

B

Explanation:

Improving employee training and awareness is the best option to address the issue of sensitive reports being disclosed via file sharing services. By educating employees about the risks of unapproved file sharing, the security protocols to follow, and the proper channels to use for sharing company information, an organization can significantly reduce the risk of sensitive data being accidentally or intentionally

shared on insecure platforms. This human-centric approach addresses the root cause of the problem. Options A, C, and D are security controls that do not directly address the behavior of sharing sensitive files on unauthorized services.

Question 11

Question Type: MultipleChoice

The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?

Options:

A- SQL01

B- WK10-Sales07

C- WK7-Plant01

D- DCEast01

E- HQAdmin9

Answer:

D

Explanation:

Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10-Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.