CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following is a reason to take a DevSecOps approach to a software assurance program?

A. To find and fix security vulnerabilities earlier in the development process

B. To speed up user acceptance testing in order to deliver the code to production faster

C. To separate continuous integration from continuous development in the SDLC

D. To increase the number of security-related bug fixes worked on by developers

Correct Answer: A

QUESTION 2

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

A. Deploy agents on all systems to perform the scans

B. Deploy a central scanner and perform non-credentialed scans

C. Deploy a cloud-based scanner and perform a network scan

D. Deploy a scanner sensor on every segment and perform credentialed scans

Correct Answer: D

QUESTION 3

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication

B. Rogue device on the network

C. Abnormal OS process behavior

D. Data exfiltration

Correct Answer: D

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect

personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls

The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat,

and that the email is used to exfiltrate data from the network to an external party.

The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

QUESTION 4

The management team has asked a senior security engineer to explore DLP security solutions for the company\\'s growing use of cloud-based storage. Which of the following is an appropriate solution to control the sensitive data that is being stored in the cloud?

A. NAC

B. IPS

C. CASB

D. WAF

Correct Answer: C

A cloud access security broker (CASB) is a security solution that monitors and controls the use of cloud-based services and applications. A CASB can provide data loss prevention (DLP) capabilities for sensitive data that is being stored in the cloud, such as encryption, masking, tokenization, or redaction. A CASB can also enforce policies and compliance requirements for cloud usage, such as authentication, authorization, auditing, and reporting. The other options are not appropriate solutions for controlling sensitive data in the cloud. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://docs.microsoft.com/en-us/cloudapp-security/what-is-cloud-app-security

QUESTION 5

A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

A. EDR

B. Port security

C. NAC

D. Segmentation

Correct Answer: A

EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all

devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are

patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance

requirements across all devices .

https://www.crowdstrike.com/epp-101/what-is-endpoint-detection-and-response-edr/

QUESTION 6

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

A. SLA

B. MOU

C. NDA

D. Limitation of liability

Correct Answer: A

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

QUESTION 7

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

A. Nmap

B. TCPDump

C. SIEM

D. EDR

Correct Answer: B

In this scenario, where the administrator suspects a DoS attack related to half-open TCP sessions consuming memory, TCPDump would be the best tool to use. It can help prove whether the server is experiencing this behavior by capturing

and analyzing the network packets to identify patterns consistent with half-open TCP sessions.

QUESTION 8

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan

B. Discovery scan

C. Vulnerability scan

D. Credentialed scan

Correct Answer: B

A discovery scan is typically used to identify the scope of a web application and understand where the scan will go. This type of scan is often the first step in assessing a web application\\'s security and helps the analyst determine which areas

should be further examined or tested in-depth.

Reference: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/scans/scanning_basics.htm

QUESTION 9

A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:

```
Source: Email filtering tool
Event: Malicious message delivered notification
ID: 1905

Source: Antivirus Solution
Event: Virus CS0-726 detected
ID: 2008

Source: Firewall
Event: Outbound connection to known-bad IP blocked
ID: 1987
```

Which of the following is the best way for the analyst to automate alert generation?

A. Deploy a signature-based IDS

B. Install a UEBA-capable antivirus

C. Implement email protection with SPF

D. Create a custom rule on a SIEM

Correct Answer: D

A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-managementsiem-implementation-33969

QUESTION 10

An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

A. A DLP system

B. DNS sinkholing

C. IP address allow list

D. An inline IDS

Correct Answer: B

DNS sinkholing is a mechanism that can prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains by returning a false or controlled IP address for those domains. This can

reduce the load on the firewall by intercepting the DNS requests before they reach the firewall and diverting them to a sinkhole server. The other options are not relevant or effective for this purpose. CompTIA Cybersecurity Analyst (CySA+)

Certification Exam Objectives (CS0-002), page 9;

https://www.enisa.europa.eu/topics/incidentresponse/glossary/dns-sinkhole

QUESTION 11

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A. Deploy a CASB and enable policy enforcement

B. Configure MFA with strict access

C. Deploy an API gateway

D. Enable SSO to the cloud applications

Correct Answer: A

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

QUESTION 12

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A. Develop a call tree to inform impacted users

B. Schedule a review with all teams to discuss what occurred

C. Create an executive summary to update company leadership

D. Review regulatory compliance with public relations for official notification

Correct Answer: B

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official https://www.eccouncil.org/cybersecurity-exchange/threatintelligence/ cyber-kill-chain-seven-steps-cyberattack/

QUESTION 13

A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

A. CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

B. CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

C. CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Correct Answer: C

Reference: https://www.first.org/cvss/specification-document

QUESTION 14

An analyst is reviewing the following output:

```
if (searchname != null)
 {
  %>
     employee <%searchname%> not found
  <%
 }
```

Vulnerability found: Improper neutralization of script-related HTML tag Which of the following was most likely used to discover this?

A. Reverse engineering using a debugger

B. A static analysis vulnerability scan

C. A passive vulnerability scan

D. A database vulnerability scan

Correct Answer: D

QUESTION 15

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. config.ini

B. ntds.dit

C. Master boot record

D. Registry

Correct Answer: D

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values. The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.