CAS-005 Q&As

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

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

https://www.geekcert.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions.

The architect discovers that the acquired companies use different vendors for detection and monitoring

The architect\\'s goal is to:

1.

Create a collection of use cases to help detect known threats

2.

Include those use cases in a centralized library for use across all of the companies

Which of the following is the best way to achieve this goal?

A. Sigma rules

B. Ariel Query Language

C. UBA rules and use cases

D. TAXII/STIX library

Correct Answer: A

To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option. Here\\'s why: Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms. Centralized Rule Management: By using Sigma rules, the cybersecurity architect can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities. Ease of Use and Flexibility: Sigma provides a structured and straightforward format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

QUESTION 2

An incident response team is analyzing malware and observes the following:

1.

Does not execute in a sandbox

2.

No network loCs

3.

No publicly known hash match

4.

No process injection method detected

Which of the following should the team do next to proceed with further analysis?

A. Use an online vims analysis tool to analyze the sample

B. Check for an anti-virtualization code in the sample

C. Utilize a new deployed machine to run the sample.

D. Search oilier internal sources for a new sample.

Correct Answer: B

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid

detection. Checking for anti-virtualization code is a logical next step because:

It helps determine if the malware is designed to evade analysis tools. Identifying such code can provide insights into the malware\\'s behavior and intent. This step can also inform further analysis methods, such as running the malware on

physical hardware.

References:

CompTIA Security+ Study Guide

SANS Institute, "Malware Analysis Techniques"

"Practical Malware Analysis" by Michael Sikorski and Andrew Honig

QUESTION 3

A security technician is trying to connect a remote site to the central office over a site-to-site VPN. The technician has verified the source and destination IP addresses are correct, but the technician is unable to get the remote site to connect. The following error message keeps repeating:

An error has occurred during Phase 1 handshake. Deleting keys and retrying...

Which of the following is most likely the reason the connection is failing?

A. The IKE hashing algorithm uses different key lengths on each VPN device.

B. The IPSec settings allow more than one cipher suite on both devices.

C. The Diffie-Hellman group on both sides matches but is a legacy group.

D. The remote VPN is attempting to connect with a protocol other than SSL/TLS.

Correct Answer: C

The error message "An error has occurred during Phase 1 handshake. Deleting keys and retrying..." suggests that there is an issue with the initial negotiation or key exchange process. Legacy Diffie-Hellman groups are a common cause of such issues because modern VPN devices might reject or fail to negotiate with older, less secure groups.

QUESTION 4

A commercial OSINT provider utilizes and reviews data from various sources of publicly available information. The provider is transitioning the subscription service to a model that limit\\'s the scope of available data based on subscription tier. Which of the following approaches would best ensure subscribers are only granted access to data associated with their tier? (Choose two.)

A. Storing collected data on separate physical media per tier

B. Controlling access to data based on the role of users

C. Employing attribute-based access control

D. Implementing a behavior-based IDS positioned at the storage network gateway

E. Establishing a classification and labeling scheme

F. Implementing a mandatory access control scheme

Correct Answer: BE

QUESTION 5

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole.

Which of the following is the best way to achieve this goal? (Select two).

A. Implementing DLP controls preventing sensitive data from leaving Company B\\'s network

B. Documenting third-party connections used by Company B

C. Reviewing the privacy policies currently adopted by Company B

D. Requiring data sensitivity labeling tor all files shared with Company B

E. Forcing a password reset requiring more stringent passwords for users on Company B\\'s network

F. Performing an architectural review of Company B\\'s network

Correct Answer: AB

To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:

A. Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure. E. Performing an architectural

review of Company B\\'s network: This review will identify vulnerabilities and assess the security posture of the acquired company\\'s network, providing a comprehensive understanding of the new attack surface. These actions will provide a

clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

References:

CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions. NIST Special Publication 800-37, "Guide for Applying the Risk Management

Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections. "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis:

Discusses the importance of security assessments during acquisitions.