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

QUESTION 1

A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic.

Which of the following should the analyst use to determine whether the requests are malicious?

A. User-agent string

B. Byte length of the request

C. Web application headers

D. HTML encoding field

Correct Answer: A

The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.

Why Use User-Agent String?

Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.

Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.

Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.

Other options provide useful information but may not be as effective for initial determination of the nature of the request:

B. Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.

C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.

D. HTML encoding field: This is not typically used for identifying the nature of the request.

References:

CompTIA SecurityX Study Guide

"User-Agent Analysis for Security," OWASP

NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

QUESTION 2

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 3

Users are willing passwords on paper because of the number of passwords needed in an environment.

Which of the following solutions is the best way to manage this situation and decrease risks?

A. Increasing password complexity to require 31 least 16 characters

B. implementing an SSO solution and integrating with applications

C. Requiring users to use an open-source password manager

D. Implementing an MFA solution to avoid reliance only on passwords

Correct Answer: B

Implementing a Single Sign-On (SSO) solution and integrating it with applications is the best way to manage the situation and decrease risks. Here\\'s why:

Reduced Password Fatigue: SSO allows users to log in once and gain access to multiple applications and systems without needing to remember and manage multiple passwords. This reduces the likelihood of users writing down passwords.

Improved Security: By reducing the number of passwords users need to manage, SSO decreases the attack surface and potential for password-related security breaches. It also allows for the implementation of stronger authentication

methods. User Convenience: SSO improves the user experience by simplifying the login process, which can lead to higher productivity and satisfaction.

References:

QUESTION 4

A company wants to implement hardware security key authentication for accessing sensitive information systems The goal is to prevent unauthorized users from gaining access with a stolen password Which of the following models should the company implement to best solve this issue?

A. Rule based

B. Time-based

C. Role based

D. Context-based

Correct Answer: D

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user\\'s current environment and behavior. This can include factors such as the user\\'s location, the time of access,

the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.

Time-based (B) authentication considers the time factor but doesn\\'t provide comprehensive protection against stolen credentials. Role-based (C) is more about access control based on the user\\'s role within the organization rather than

authenticating the user based on current context. By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is

unlikely to possess) provide a robust defense mechanism.

References:

CompTIA SecurityX guide on authentication models and best practices. NIST guidelines on authentication and identity proofing. Analysis of multi-factor and adaptive authentication techniques.

QUESTION 5

While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter.

Which of the following best describes this type of correlation?

A. Spear-phishing campaign

B. Threat modeling

C. Red team assessment

D. Attack pattern analysis

Correct Answer: A

The situation where several employees were contacted by the same individual impersonating a recruiter best describes a spear-phishing campaign. Here\\'s why:

Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.

Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spear-phishing to gain the trust of the targeted individuals and increase the likelihood of a successful attack. Correlated Contacts: The fact that several

employees were contacted by the same individual suggests a coordinated effort to breach the organization\\'s security by targeting multiple points of entry through social engineering.