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.geekcert.com/cs0-003.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 security analyst performs a weekly vulnerability scan on a network that has 240 devices and receives a report with 2.450 pages. Which of the following would most likely decrease the number of false positives?

A. Manual validation

B. Penetration testing

C. A known-environment assessment

D. Credentialed scanning

Correct Answer: D

Credentialed scanning is a method of vulnerability scanning that uses valid user credentials to access the target systems and perform a more thorough and accurate assessment of their security posture. Credentialed scanning can help to reduce the number of false positives by allowing the scanner to access more information and resources on the systems, such as configuration files, registry keys, installed software, patches, and permissions . https://www.tenable.com/blog/credentialed-vulnerability-scanning-what-why-and-how

QUESTION 2

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

A. SOAR

B. SIEM

C. SLA

D. IoC

Correct Answer: A

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

QUESTION 3

An analyst needs to understand how an attacker compromised a server. Which of the following procedures will best deliver the information that is necessary to reconstruct the steps taken by the attacker?

A. Scan the affected system with an anti-malware tool and check for vulnerabilities with a vulnerability scanner.

B. Extract the server\\'s system timeline, verifying hashes and network connections during a certain time frame.

C. Clone the entire system and deploy it in a network segment built for tests and investigations while monitoring the system during a certain time frame.

D. Clone the server\\'s hard disk and extract all the binary files, comparing hash signatures with malware databases.

Correct Answer: B

QUESTION 4

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.

QUESTION 5

A company\\'s legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur. The department has asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the best way to achieve this goal?

A. Focus on incidents that have a high chance of reputation harm.

B. Focus on common attack vectors first.

C. Focus on incidents that affect critical systems.

D. Focus on incidents that may require law enforcement support.

Correct Answer: B

Latest CS0-003 Dumps CS0-003 PDF Dumps CS0-003 Exam Questions