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.leads4pass.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

A Chief Information Security Officer is concerned that contract developers may be able to steal the code used to design the company\\'s latest application since they are able to pull code from a cloud-based repository directly to laptops that are not owned by the company. Which of the following solutions would best protect the company code from being stolen?

A. MDM

B. SCA

C. CASB

D. VDI

Correct Answer: D

VDI provides a secure environment for accessing company resources, such as code repositories, from remote locations. With VDI, the code repository would be accessed through a virtual desktop hosted on the company\\'s servers, rather than on the developer\\'s laptop. This means that the company\\'s IT department can control the virtual desktop and ensure that it is secure, including installing security software, monitoring activity, and limiting access to the code repository.

QUESTION 2

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 3

A cybersecurity analyst is working with a SIEM tool and reviewing the following table:

Risk level	Asset type	Environment	Network zone	Vulnerability score
High	Critical	Production	DMZ	5
	Important	Production	DMZ	
	Ordinary	Production	DMZ	
Medium	Critical	Production	DMZ	4
	Critical	Production	LAN	
	Important	Production	LAN	
	Ordinary	Production	LAN	
Low	Critical	Non-production	LAN	3
	Critical	Production	LAN	
	Important	Non-production	DMZ	
	Ordinary	Non-production	LAN	
Informational	Critical	Non-production	DMZ	1–2
	Critical	Production	LAN	
	Important	Non-production	LAN	
	Ordinary	Non-production	LAN	

When creating a rule in the company\\'s SIEM, which of the following would be the BEST approach for the analyst to use to assess the risk level of each vulnerability that is discovered by the vulnerability assessment tool?

A. Create a trend with the table and join the trend with the desired rule to be able to extract the risk level of each vulnerability

B. Use Boolean filters in the SIEM rule to take advantage of real-time processing and RAM to store the table dynamically, generate the results faster, and be able to display the table in a dashboard or export it as a report

C. Use a static table stored on the disk of the SIEM system to correlate its data with the data ingested by the vulnerability scanner data collector

D. Use the table as a new index or database for the SIEM to be able to use multisearch and then summarize the results as output

Correct Answer: B

QUESTION 4

A. Deploy a database to aggregate the logging

B. Configure the servers to forward logs to a SIEM

C. Share the log directory on each server to allow local access.

D. Automate the emailing of logs to the analysts.

Correct Answer: B

The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.

A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from

various sources across an organization\\'s network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate

cyberattacks.

By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can

save time, improve efficiency, and enhance security posture.

Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access © may not be scalable or secure for a large

number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

QUESTION 5

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline

B. Evidence

C. Impact

D. Scope

Correct Answer: C

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service.The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.