CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.geekcert.com/cs0-002.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

Which of the following is a difference between SOAR and SCAP?

A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics

B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope

C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does

D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts

Correct Answer: B

QUESTION 2

A company\\'s blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.

B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.

C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.

D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.

Correct Answer: D

This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

QUESTION 3

A company\\'s legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

A. VDI

B. SaaS

C. CASB

D. FaaS

Correct Answer: B

Which of the follawing activities is designed to handle a control failure that leads to a breach? Risk assessment Incident management Root cause analysis Vulnerability management Software as a Service (SaaS) -Provides all the hardware, operating system, software, and applications needed for a complete application service to be delivered -Cloud service providers are responsible for the security of the platform and infrastructure -Consumers are responsible for application security, account provisioning, and authorizations

Cloud Access Security Broker (CASB)

-Enterprise management software designed to mediate access to cloud services by users across all types of devices Single sign-on Malware and rogue device detection Monitor/audit user activity Mitigate data exfiltration

-Cloud Access Service Brokers provide visibility into how clients and another network nodes use cloud services Forward Proxy Reverse Proxy API

QUESTION 4

A security analyst is concerned that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst\\'s concern?

A. LDAPS

B. MFA

C. SAML

D. SHA-1

Correct Answer: C

Reference: https://www.varonis.com/blog/what-is-saml

QUESTION 5

An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

A. MAC

B. TAP

C. NAC

D. ACL

Correct Answer: C

CS0-002 VCE Dumps CS0-002 Study Guide CS0-002 Braindumps