Free Questions for 350-201 by go4braindumps

Shared by Austin on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An analyst received multiple alerts on the SIEM console of users that are navigating to malicious URLs. The analyst needs to automate the task of receiving alerts and processing the data for further investigations. Three variables are available from the SIEM console to include in an automation script: console_ip, api_token, and reference_set_name. What must be added to this script to receive a successful HTTP response?

#!/usr/bin/python import sys import requests

Options:

A- {1}, {2}

B- {1}, {3}

C- console_ip, api_token

D- console_ip, reference_set_name

Answer:

C

Question 2

Question Type: MultipleChoice

What is the difference between process orchestration and automation?

Options:

A- Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.

B- Orchestration arranges the tasks, while automation arranges processes.

C- Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.

D- Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.

Answer:

A

Question 3

Question Type: MultipleChoice

What is the impact of hardening machine images for deployment?

Options:

A- reduces the attack surface

B- increases the speed of patch deployment

C- reduces the steps needed to mitigate threats

D- increases the availability of threat alerts

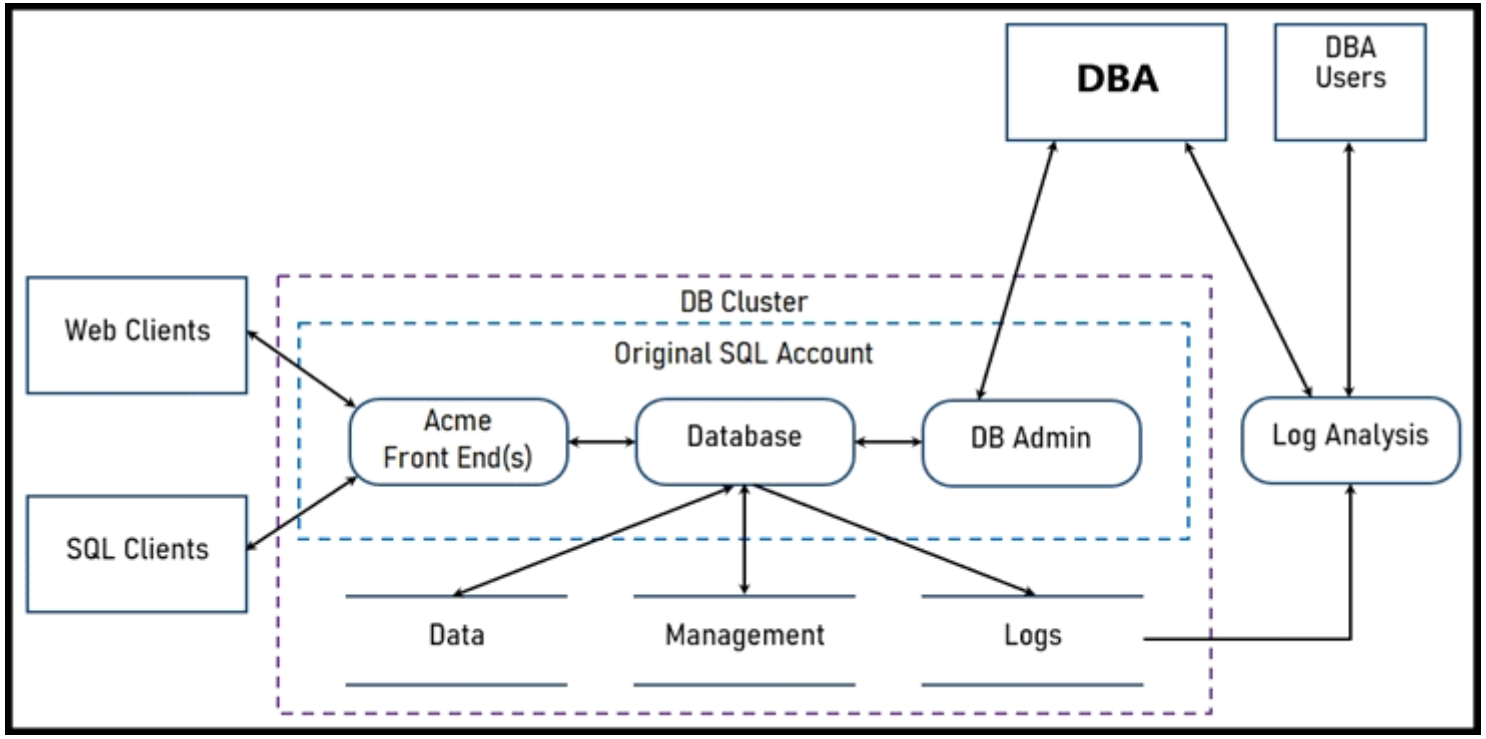
Answer:

A

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.



Two types of clients are accessing the front ends and the core database that manages transactions, access control, and atomicity. What is the threat model for the SQL database?

Options:

A- An attacker can initiate a DoS attack.

B- An attacker can read or change data.

C- An attacker can transfer data to an external server.

D- An attacker can modify the access logs.

Answer:

A

Question 5

Question Type: **MultipleChoice**

An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to

prevent this type of attack from reoccurring? (Choose two.)

Options:

A- Implement a patch management process.

B- Scan the company server files for known viruses.

C- Apply existing patches to the company servers.

D- Automate antivirus scans of the company servers.

E- Define roles and responsibilities in the incident response playbook.

Answer:

D, E

Question 6

Question Type: **MultipleChoice**

A security architect in an automotive factory is working on the Cyber Security Management System and is implementing procedures and creating policies to prevent attacks. Which standard must the architect apply?

Options:

A- IEC62446

B- IEC62443

C- IEC62439-3

D- IEC62439-2

Answer:

B

To Get Premium Files for 350-201 Visit

https://www.p2pexams.com/products/350-201

For More Free Questions Visit

https://www.p2pexams.com/cisco/pdf/350-201