350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

QUESTION 1

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/pythonimport sysimport requests

A. {1}, {2}

B. {1}, {3}

C. console_ip, api_token

D. console_ip, reference_set_name

Correct Answer: C

QUESTION 2

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected.

What action should be taken to harden the network?

A. Move the IPS to after the firewall facing the internal network

B. Move the IPS to before the firewall facing the outside network

C. Configure the proxy service on the IPS

D. Configure reverse port forwarding on the IPS

Correct Answer: C

QUESTION 3

An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since deploying certificates and tracking them requires searching server owners manually.

Which action will improve workflow automation?

A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.

B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.

C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.

D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.

Correct Answer: C

QUESTION 4

An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials.

How should the workflow be improved to resolve these issues?

A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts

B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats

C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts

D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Correct Answer: B

QUESTION 5

A security incident affected an organization\\'s critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

A. Configure shorter timeout periods.

B. Determine API rate-limiting requirements.

C. Implement API key maintenance.

D. Automate server-side error reporting for customers.

E. Decrease simultaneous API responses.

Correct Answer: BD

QUESTION 6

An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

A. HIPAA

B. FISMA

C. COBIT

D. PCI DSS

Correct Answer: D

Reference: https://upserve.com/restaurant-insider/restaurant-pos-pci-compliance-checklist/

QUESTION 7

The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource.

What is the next step?

A. Conduct a risk assessment of systems and applications

B. Isolate the infected host from the rest of the subnet

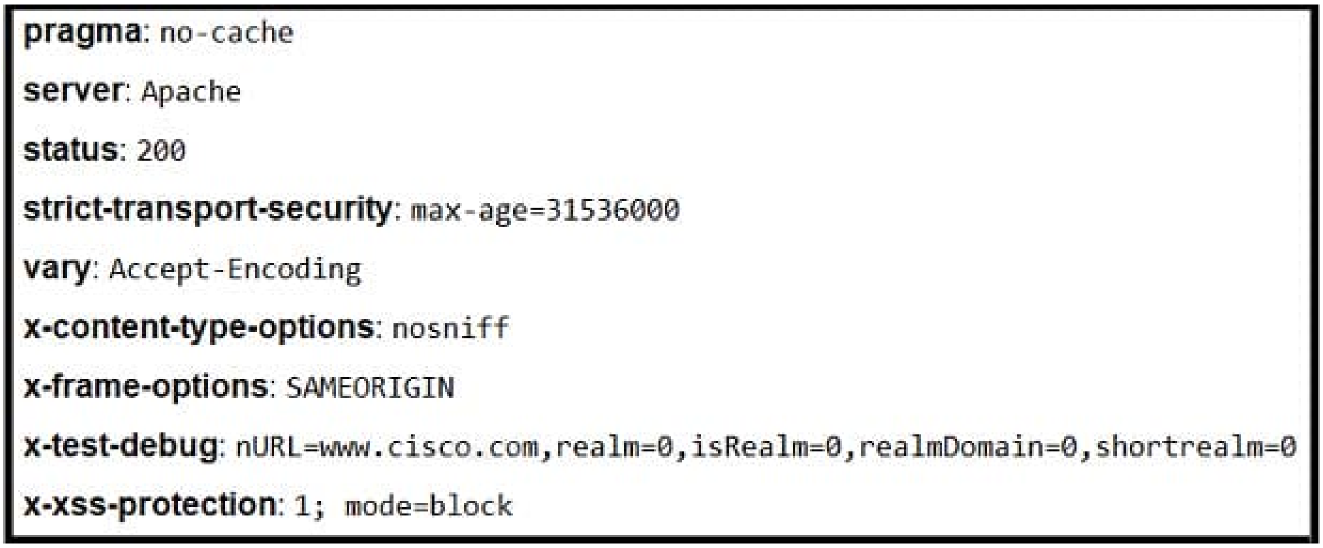
C. Install malware prevention software on the host

D. Analyze network traffic on the host\\'s subnet

Correct Answer: B

QUESTION 8

Refer to the exhibit. Where is the MIME type that should be followed indicated?



```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com,realm=0,isRealm=0,realmDomain=0,shortrealm=0
x-xss-protection: 1; mode=block
```

A. x-test-debug

B. strict-transport-security

C. x-xss-protection

D. x-content-type-options

Correct Answer: A

QUESTION 9

The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?

A. eradication and recovery

B. post-incident activity

C. containment

D. detection and analysis

Correct Answer: A

QUESTION 10

What is the difference between process orchestration and automation?

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.

Correct Answer: A

QUESTION 11

Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)

A. Evaluate the intrusion detection system alerts to determine the threat source and attack surface.

B. Communicate with employees to determine who opened the link and isolate the affected assets.

C. Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.

D. Review the mail server and proxy logs to identify the impact of a potential breach.

E. Check the email header to identify the sender and analyze the link in an isolated environment.

Correct Answer: CE

QUESTION 12

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

A. incident response playbooks

B. asset vulnerability assessment

C. report of staff members with asset relations

D. key assets and executives

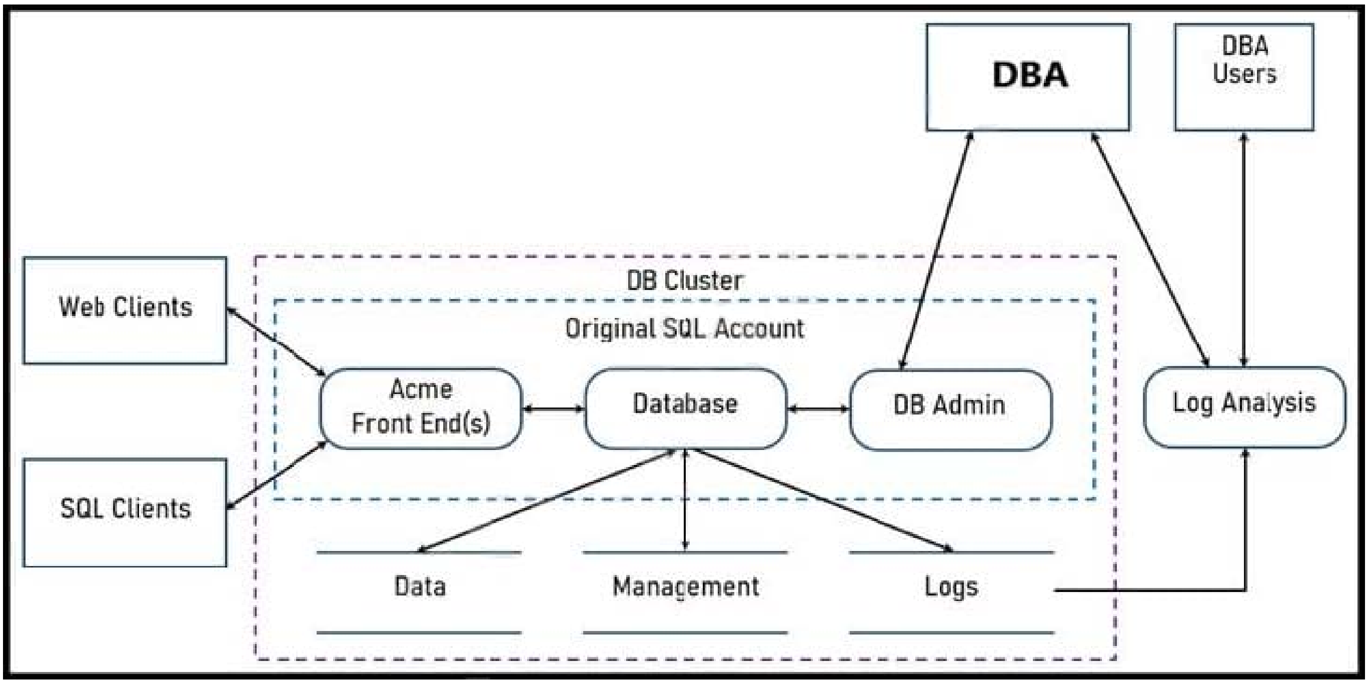
E. malware analysis report

Correct Answer: BE

Reference: https://cloudogre.com/risk-assessment/

QUESTION 13

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?



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.

Correct Answer: A

[350-201 VCE Dumps](#) [350-201 Practice Test](#) [350-201 Braindumps](#)