QUESTION 126
What is idempotence?

A. the assurance of system uniformity throughout the whole delivery process
B. the ability to recover from failures while keeping critical services running
C. the necessity of setting maintenance of individual deployment environments
D. the ability to set the target environment configuration regardless of the starting state

Answer: A

QUESTION 127
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?

A. IEC62446
B. IEC62443
C. IEC62439-3
D. IEC62439-2

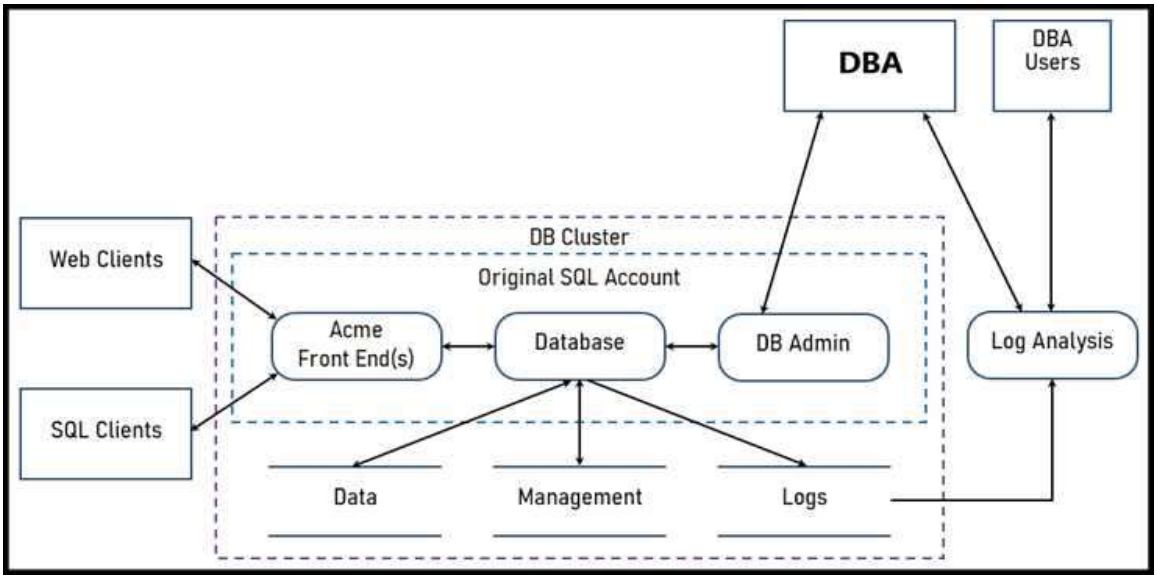
Answer: B

QUESTION 128
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.)

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: DE

QUESTION 129
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.

Answer: A

QUESTION 130
Which bash command will print all lines from the "colors.txt" file containing the non case-sensitive pattern "Yellow"?

A. grep -i "yellow" colors.txt
B. locate "yellow" colors.txt
C. locate -i "Yellow" colors.txt
D. grep "Yellow" colors.txt

Answer: A

QUESTION 131
An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal dat

A. Which type of attack is occurring?
B. Address Resolution Protocol poisoning
C. session hijacking attack
D. teardrop attack
E. Domain Name System poisoning

Answer: D

QUESTION 132
Refer to the exhibit. An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?

```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpWebRequest.Proxy = null;
httpWebRequest.Timeout = 10000;
using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
{
    using (Stream responseStream = httpWebResponse.GetRepsonseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDocument = new XmlDocument();
            xmlDocument.LoadXml(xml);
            string innerXml = xmlDocument.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDocument.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDocument.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDocument.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDocument.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDocument.SelectSingleNode("Response//TimeZone").InnerXml;
```

A. The file is redirecting users to a website that requests privilege escalations from the user.
B. The file is redirecting users to the website that is downloading ransomware to encrypt files.
C. The file is redirecting users to a website that harvests cookies and stored account information.
D. The file is redirecting users to a website that is determining users' geographic location.

Answer: D

QUESTION 133
A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?

A. Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.
B. Inform the user by enabling an automated email response when the rule is triggered.
C. Inform the incident response team by enabling an automated email response when the rule is triggered.
D. Create an automation script for blocking URLs on the firewall when the rule is triggered.

Answer: A

QUESTION 134
A cloud engineer needs a solution to deploy applications on a cloud without being able to manage and control the server OS. Which type of cloud environment should be used?

A. IaaS
B. PaaS
C. DaaS
D. SaaS

Answer: A

QUESTION 135
Engineers are working to document, list, and discover all used applications within an organization. During the regular assessment of applications from the HR backup server, an engineer discovered an unknown application. The analysis showed that the application is communicating with external addresses on a non- secure, unencrypted channel. Information gathering revealed that the unknown application does not have an owner and is not being used by a business unit. What are the next two steps the engineers should take in this investigation? (Choose two.)

A. Determine the type of data stored on the affected asset, document the access logs, and engage

the incident response team.
B. Identify who installed the application by reviewing the logs and gather a user access log from the HR department.
C. Verify user credentials on the affected asset, modify passwords, and confirm available patches and updates are installed.
D. Initiate a triage meeting with department leads to determine if the application is owned internally or used by any business unit and document the asset owner.

Answer: AD

QUESTION 136
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.

Answer: BD

QUESTION 137
What is the impact of hardening machine images for deployment?

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 138
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.

Answer: A

QUESTION 139
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

A. {1}, {2}

B. {1}, {3}
C. console_ip, api_token
D. console_ip, reference_set_name

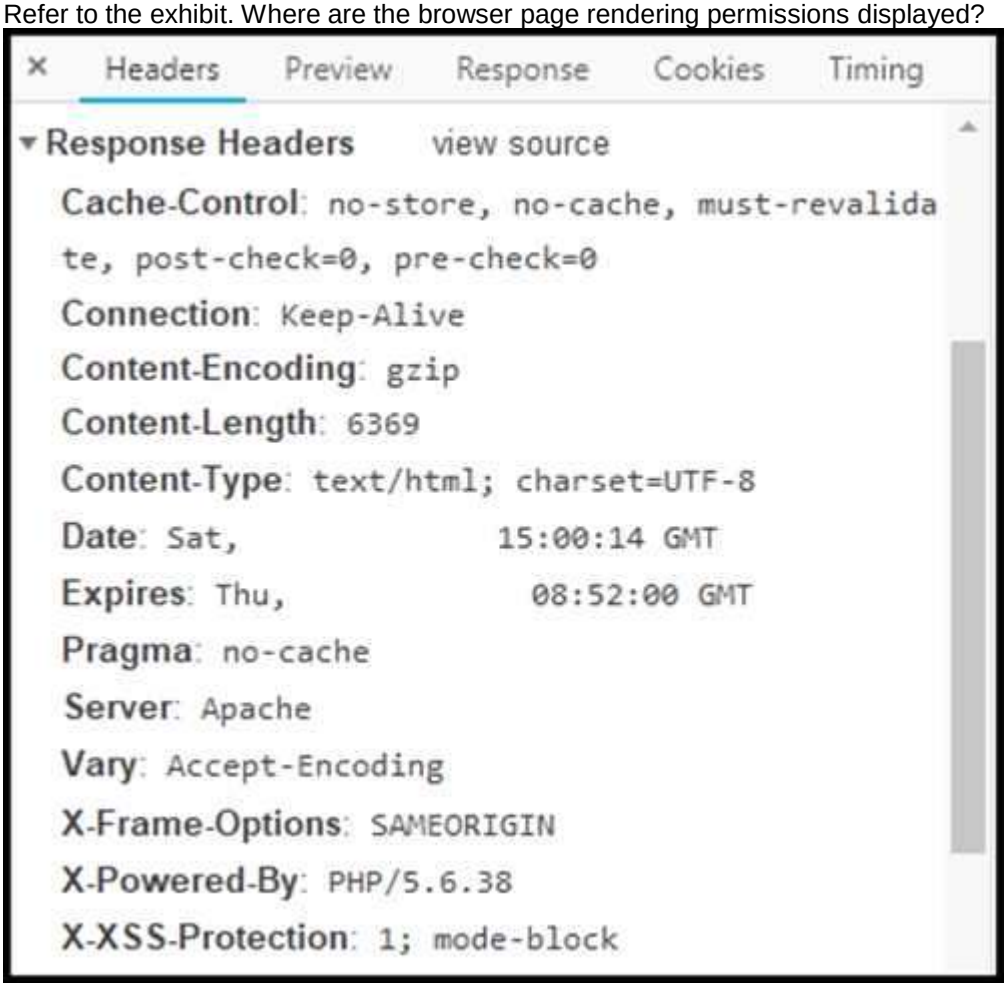
Answer: C

QUESTION 140
After a recent malware incident, the forensic investigator is gathering details to identify the breach and causes. The investigator has isolated the affected workstation. What is the next step that should be taken in this investigation?

A. Analyze the applications and services running on the affected workstation.
B. Compare workstation configuration and asset configuration policy to identify gaps.
C. Inspect registry entries for recently executed files.
D. Review audit logs for privilege escalation events.

Answer: C

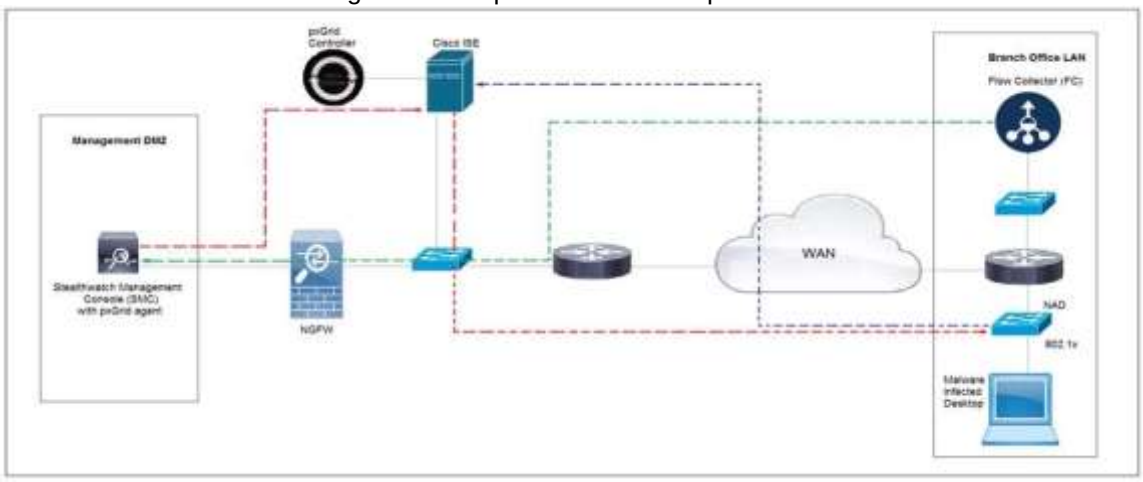
QUESTION 141
Refer to the exhibit. Where are the browser page rendering permissions displayed?



A. X-Frame-Options
B. X-XSS-Protection
C. Content-Type
D. Cache-Control

Answer: C

QUESTION 142
Refer to the exhibit. Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a quarantine VLAN using Adaptive Network Control policy.
Which method was used to signal ISE to quarantine the endpoints?



A. SNMP
B. syslog
C. REST API
D. pxGrid

Answer: C