Cisco

Exam Questions 350-201

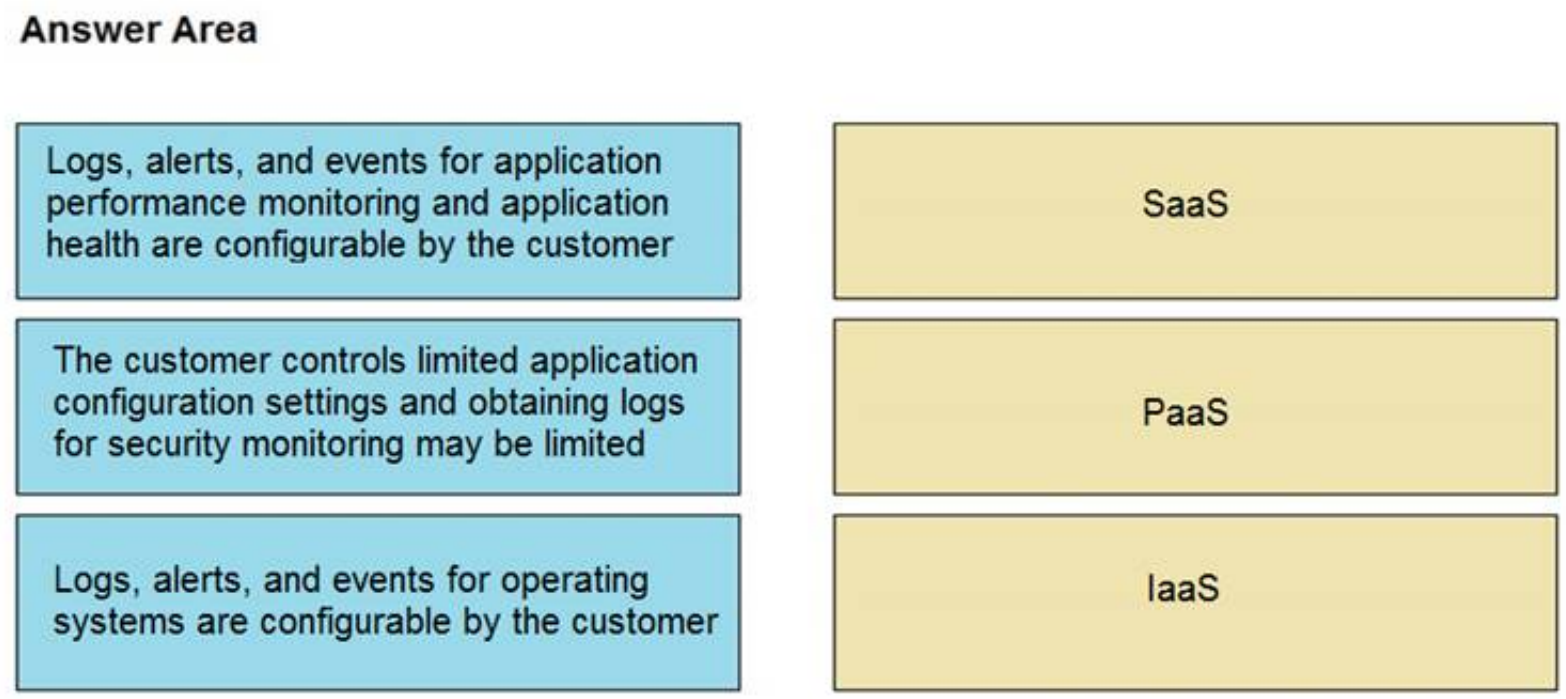
Performing CyberOps Using Core Security Technologies (CBRCOR)

NEW QUESTION 1
A patient views information that is not theirs when they sign in to the hospital's online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time. What is the first step the analyst should take to address this incident?

A. Evaluate visibility tools to determine if external access resulted in tampering
B. Contact the third-party handling provider to respond to the incident as critical
C. Turn off all access to the patient portal to secure patient records
D. Review system and application logs to identify errors in the portal code

Answer: C

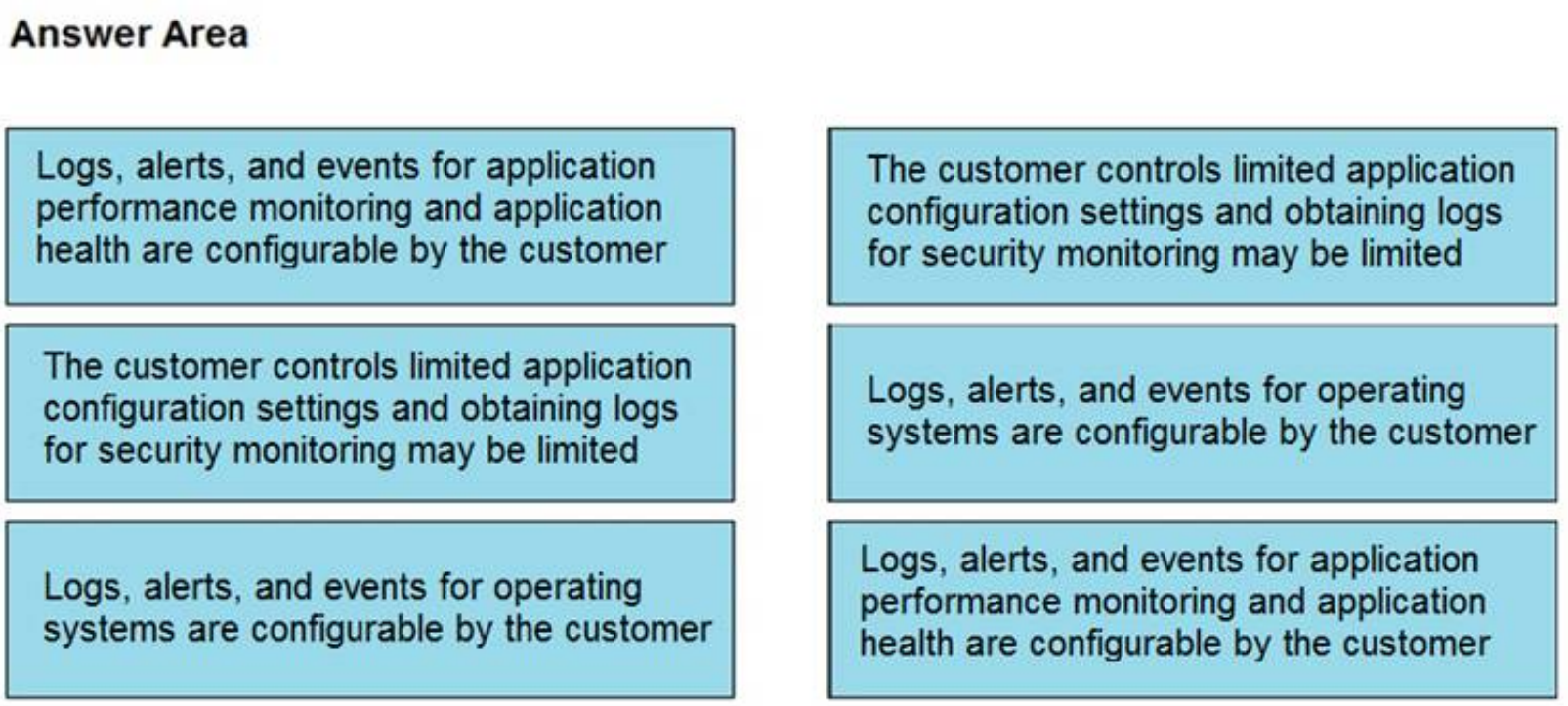
NEW QUESTION 2
Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 3
An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

A. phishing
B. dumpster diving
C. social engineering
D. privilege escalation

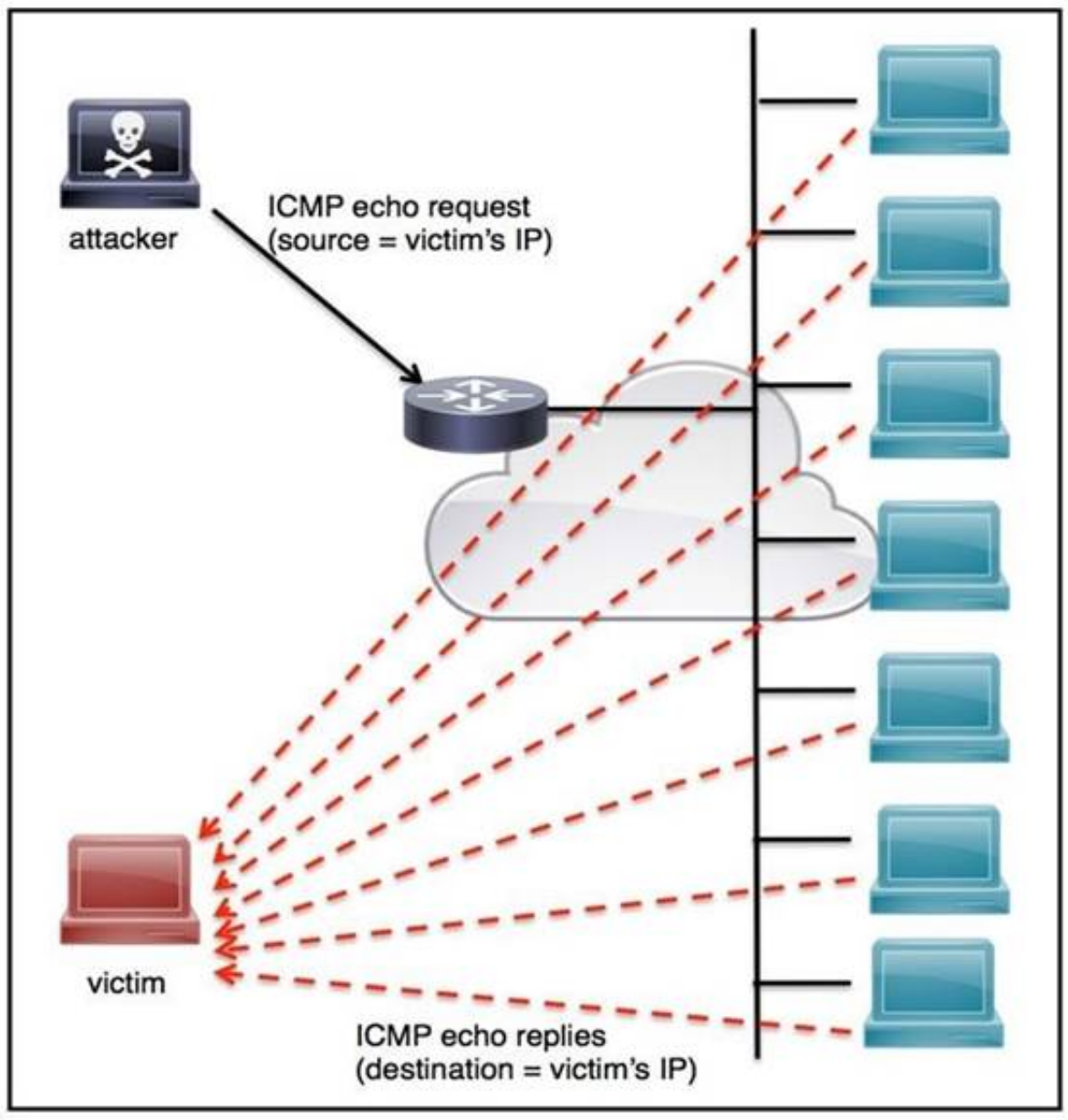
Answer: C

NEW QUESTION 4
The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

A. Contain the malware
B. Install IPS software
C. Determine the escalation path
D. Perform vulnerability assessment

Answer: D

NEW QUESTION 5
Refer to the exhibit.



An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action does the engineer recommend?

A. Use command ip verify reverse-path interface
B. Use global configuration command service tcp-keepalives-out
C. Use subinterface command no ip directed-broadcast
D. Use logging trap 6

Answer: A

NEW QUESTION 6
Refer to the exhibit.

URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

A. exploitation
B. actions on objectives
C. delivery
D. reconnaissance

Answer: C

NEW QUESTION 7
What do 2xx HTTP response codes indicate for REST APIs?

A. additional action must be taken by the client to complete the request
B. the server takes responsibility for error status codes
C. communication of transfer protocol-level information
D. successful acceptance of the client's request

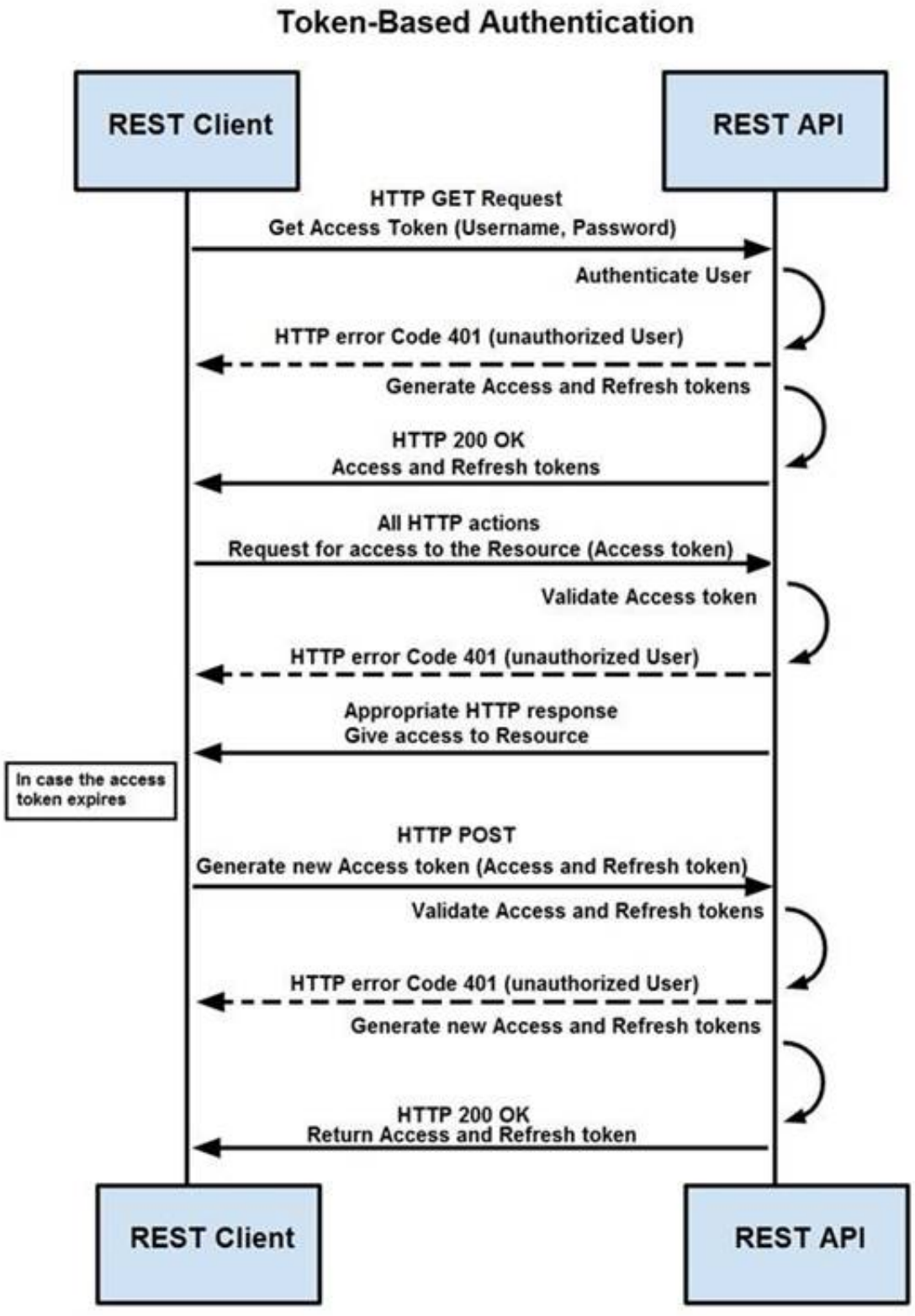
Answer: D

NEW QUESTION 8
According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

A. Perform a vulnerability assessment
B. Conduct a data protection impact assessment
C. Conduct penetration testing
D. Perform awareness testing

Answer: B

NEW QUESTION 9
Refer to the exhibit.



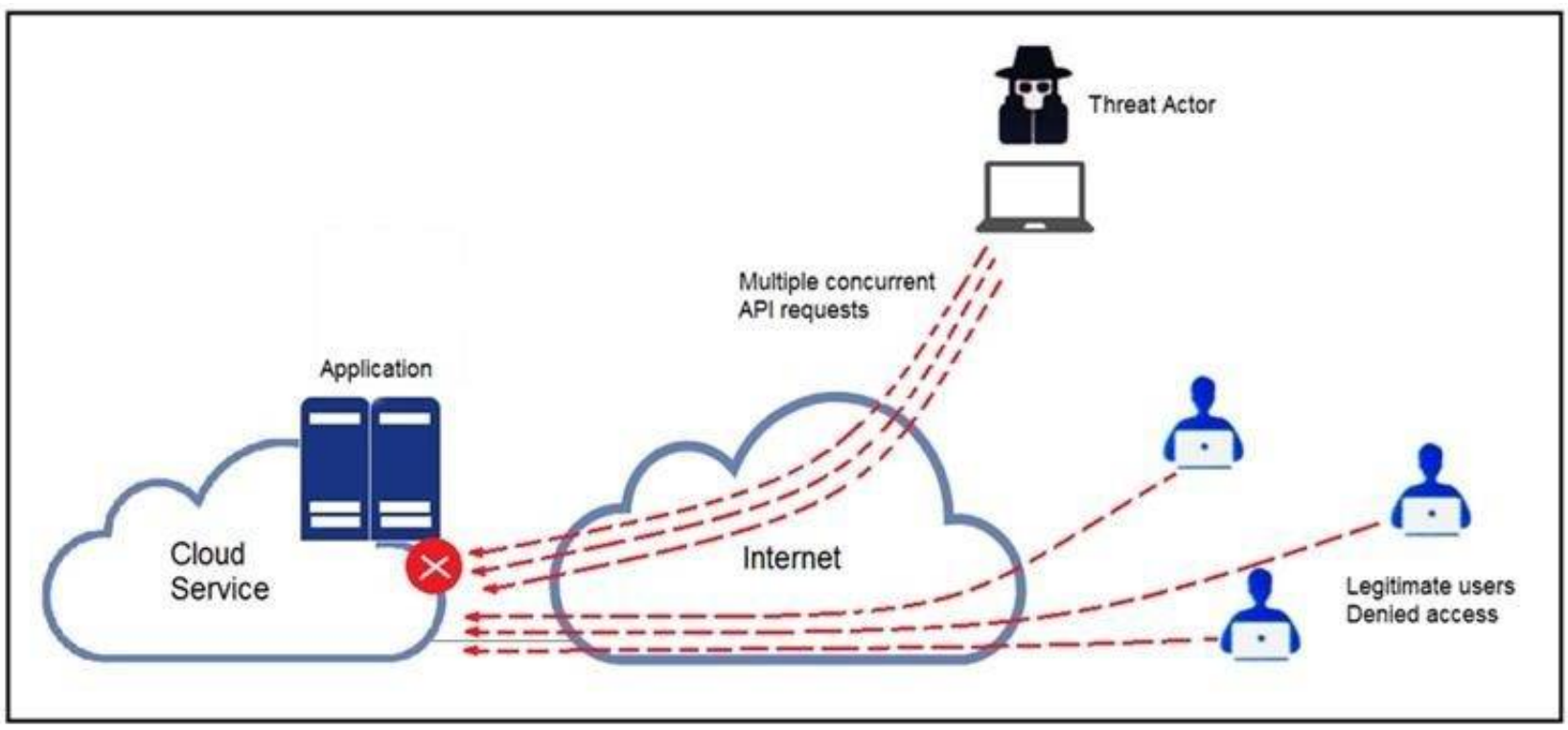
How are tokens authenticated when the REST API on a device is accessed from a REST API client?

A. The token is obtained by providing a passwor
B. The REST client requests access to a resource using the access toke
C. The REST API validates the access token and gives access to the resource.
D. The token is obtained by providing a passwor
E. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.
F. The token is obtained before providing a passwor
G. The REST API provides resource access, refreshes tokens, and returns them to the REST clien
H. The REST client requests access to a resource using theaccess token.
I. The token is obtained before providing a passwor

J. The REST client provides access to a resource using the access toke
K. The REST API encrypts the access token and gives access to the resource.

Answer: D

NEW QUESTION 10
Refer to the exhibit.



A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?

A. Limit the number of API calls that a single client is allowed to make
B. Add restrictions on the edge router on how often a single client can access the API
C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API
D. Increase the application cache of the total pool of active clients that call the API

Answer: A

NEW QUESTION 10
What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface
B. to create the logic that triggers alerts when anomalies occur
C. to identify vulnerabilities within an operating system
D. to analyze attacks to identify threat actors and points of entry

Answer: A

NEW QUESTION 13
An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies
B. exfiltration during data transfer
C. attack using default accounts
D. data exposure from backups

Answer: B

NEW QUESTION 14
An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates
B. Update the IDS/IPS signatures and reimage the affected hosts
C. Identify the systems that have been affected and tools used to detect the attack
D. Identify the traffic with data capture using Wireshark and review email filters

Answer: C

NEW QUESTION 16
Drag and drop the cloud computing service descriptions from the left onto the cloud service categories on the right.

Answer Area

triggers a block of code when triggered by a specific event	SaaS
allows renting full servers or virtual machines	PaaS
focuses on developing, testing, and delivering applications	IaaS
allows hosting and managing a virtual environment	FaaS

A. Mastered
B. Not Mastered

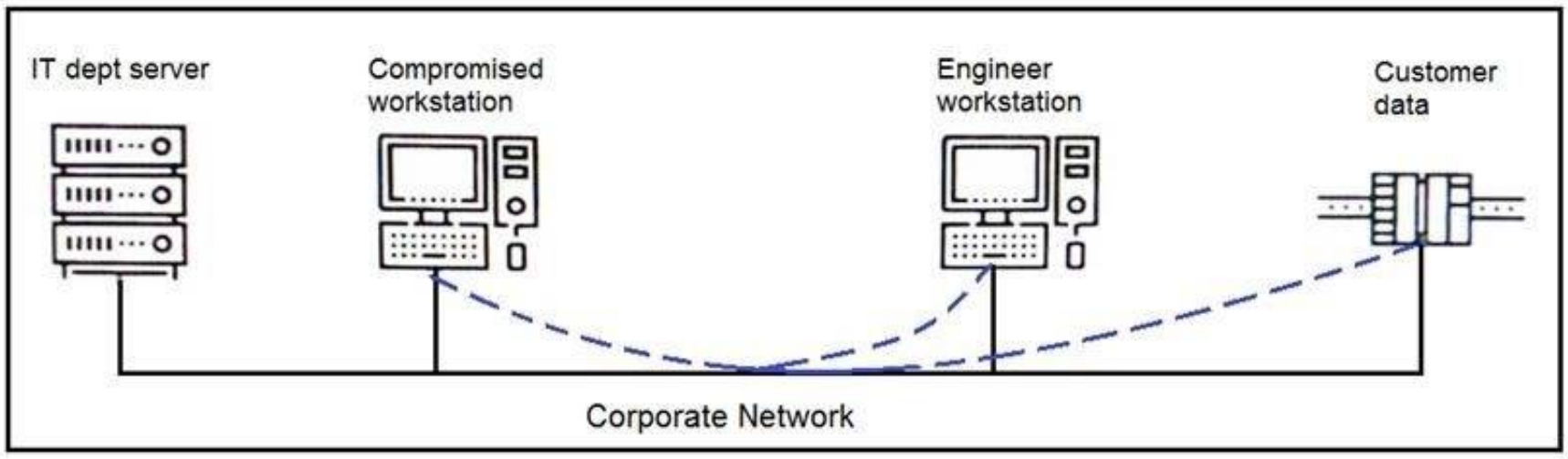
Answer: A

Explanation:

Answer Area

triggers a block of code when triggered by a specific event	focuses on developing, testing, and delivering applications
allows renting full servers or virtual machines	allows hosting and managing a virtual environment
focuses on developing, testing, and delivering applications	allows renting full servers or virtual machines
allows hosting and managing a virtual environment	triggers a block of code when triggered by a specific event

NEW QUESTION 21
Refer to the exhibit.



An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols
B. Deploy a SOAR solution and correlate log alerts from customer zones
C. Deploy IDS within sensitive areas and continuously update signatures
D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Answer: A

NEW QUESTION 25
What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

A. 401B.-402C.403D.404E.405

Answer: A

NEW QUESTION 30

Refer to the exhibit.

```
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,realDomain=0,shortrealm=0
x-xss-protection: 1; mode=block
```

Where are the browser page rendering permissions displayed?

A. x-frame-options
B. x-xss-protection
C. x-content-type-options
D. x-test-debug

Answer: C

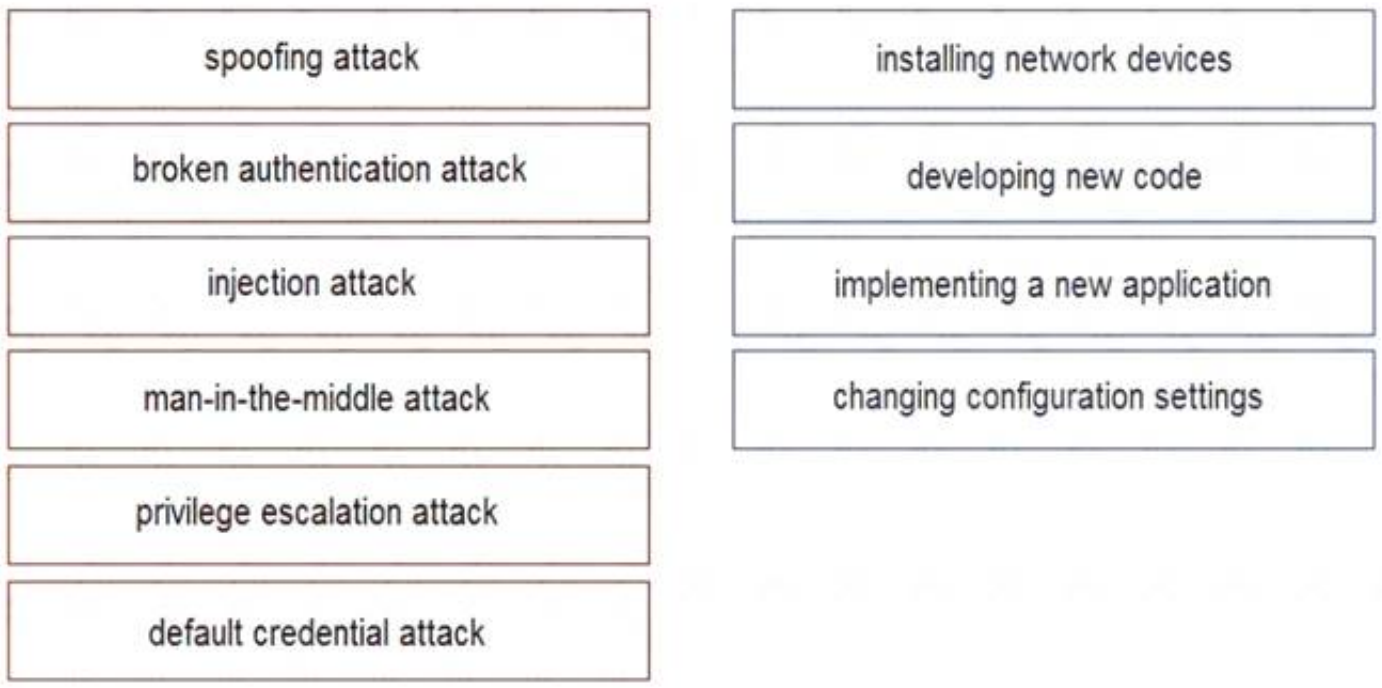
NEW QUESTION 32
A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network. What is the next step in handling the incident?

A. Block the source IP from the firewall
B. Perform an antivirus scan on the laptop
C. Identify systems or services at risk
D. Identify lateral movement

Answer: C

NEW QUESTION 36
Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Answer Area



A. Mastered
B. Not Mastered

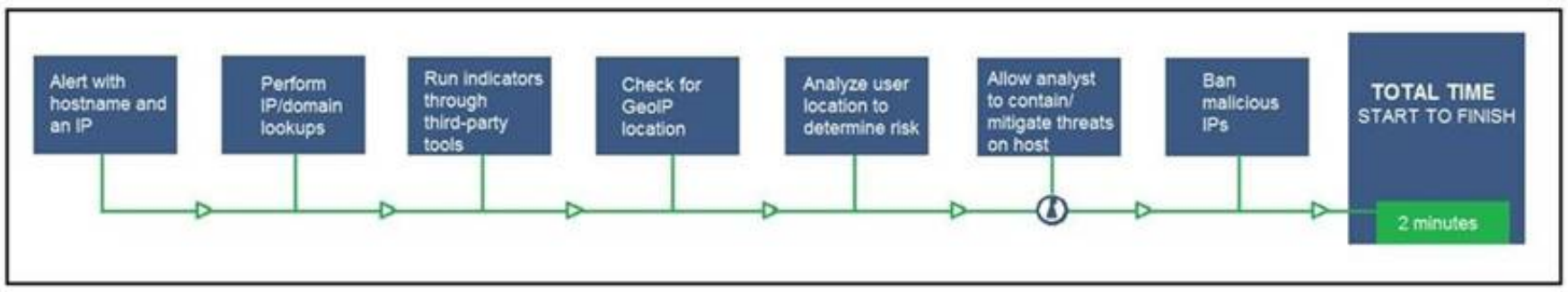
Answer: A

Explanation:

Answer Area

spoofing attack	man-in-the-middle attack
broken authentication attack	injection attack
injection attack	privilege escalation attack
man-in-the-middle attack	default credential attack
privilege escalation attack	
default credential attack	

NEW QUESTION 38
Refer to the exhibit.



An engineer configured this SOAR solution workflow to identify account theft threats and privilege escalation, evaluate risk, and respond by resolving the threat. This solution is handling more threats than Security analysts have time to analyze. Without this analysis, the team cannot be proactive and anticipate attacks. Which action will accomplish this goal?

A. Exclude the step “BAN malicious IP” to allow analysts to conduct and track the remediation
B. Include a step “Take a Snapshot” to capture the endpoint state to contain the threat for analysis
C. Exclude the step “Check for GeoIP location” to allow analysts to analyze the location and the associated risk based on asset criticality
D. Include a step “Reporting” to alert the security department of threats identified by the SOAR reporting engine

Answer: A

NEW QUESTION 42
An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

A. Restrict the number of requests based on a calculation of daily average
B. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
C. Implement REST API Security Essentials solution to automatically mitigate limit exhaustio
D. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
E. Increase a limit of replies in a given interval for each AP
F. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
G. Apply a limit to the number of requests in a given time interval for each AP
H. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D

NEW QUESTION 47
An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

A. ExecutedMalware.ioc
B. Crossrider.ioc
C. ConnectToSuspiciousDomain.ioc
D. W32 AccesschkUtility.ioc

Answer: D

NEW QUESTION 52

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu
B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu
C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu
D. Discovery, System Network Configuration Discovery, Duqu

Answer: A

NEW QUESTION 53
A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server. Which security solution is needed at this stage to mitigate the attack?

A. web security solution
B. email security solution
C. endpoint security solution
D. network security solution

Answer: D

NEW QUESTION 58
Refer to the exhibit.

Vulnerability #1	Vulnerability #2
A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions: a) Be logged in to the device over telnet or SSH, or through the local console b) Be logged in as a high-privileges administrative user In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device. All software versions are affected Fixes are available now There are no workarounds or mitigations	A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to: a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack. All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.

How must these advisories be prioritized for handling?

A. The highest priority for handling depends on the type of institution deploying the devices
B. Vulnerability #2 is the highest priority for every type of institution
C. Vulnerability #1 and vulnerability #2 have the same priority
D. Vulnerability #1 is the highest priority for every type of institution

Answer: D

NEW QUESTION 62
Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Answer Area

not visible to the victim	reconnaissance
virus scanner turning off	weaponization
malware placed on the targeted system	delivery
open port scans and multiple failed logins from the website	exploitation
large amount of data leaving the network through unusual ports	installation
system phones connecting to countries where no staff are located	command & control
USB with infected files inserted into company laptop	actions on objectives

A. Mastered
B. Not Mastered

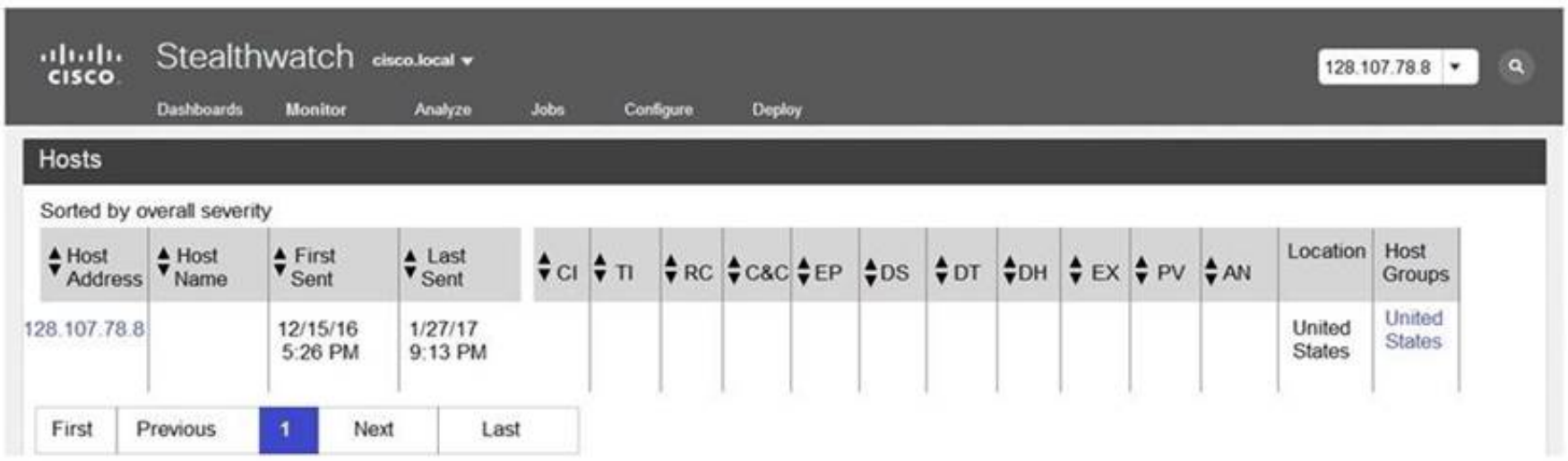
Answer: A

Explanation:

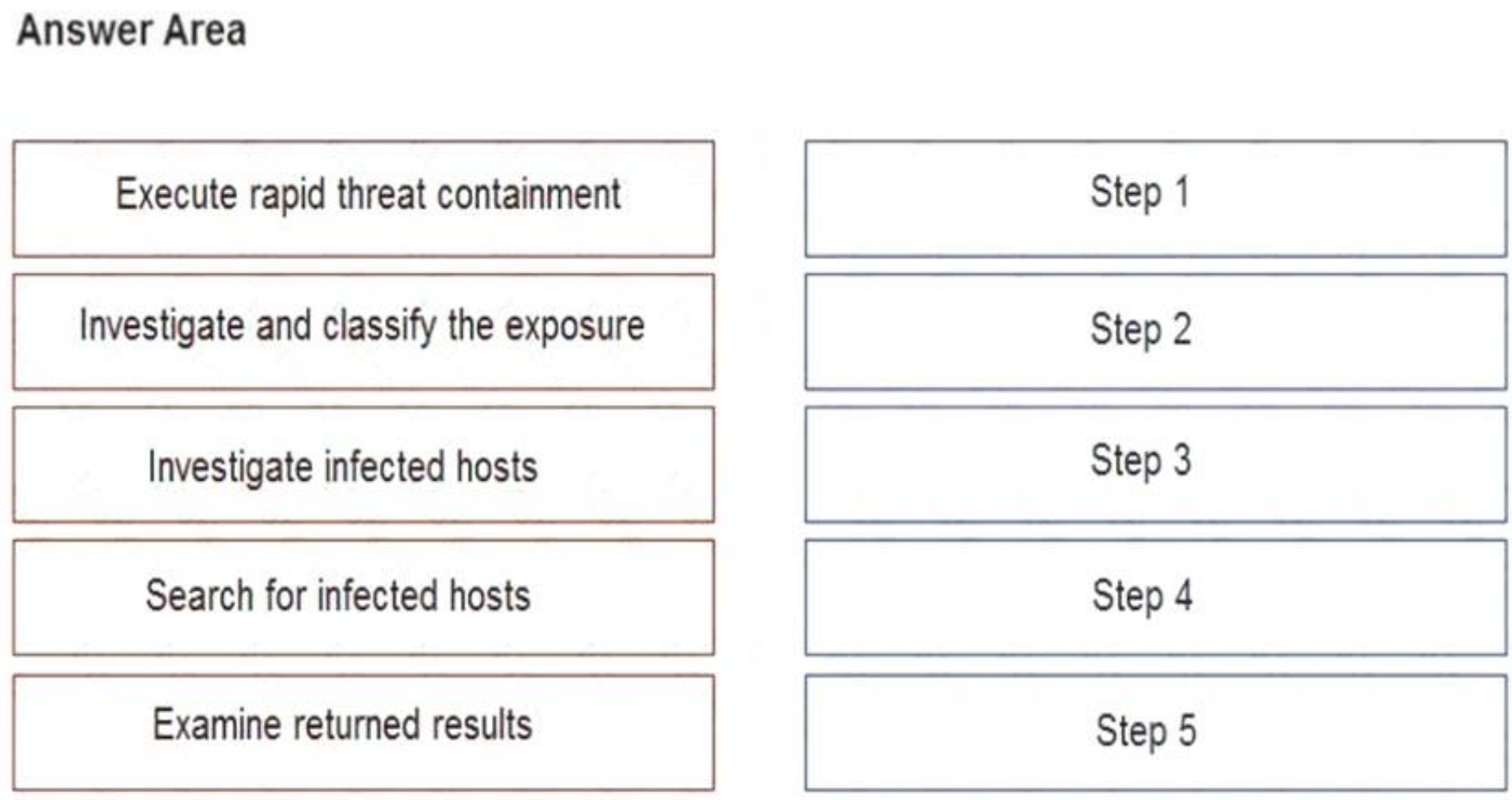
Answer Area

not visible to the victim	system phones connecting to countries where no staff are located
virus scanner turning off	malware placed on the targeted system
malware placed on the targeted system	not visible to the victim
open port scans and multiple failed logins from the website	large amount of data leaving the network through unusual ports
large amount of data leaving the network through unusual ports	USB with infected files inserted into company laptop
system phones connecting to countries where no staff are located	virus scanner turning off
USB with infected files inserted into company laptop	open port scans and multiple failed logins from the website

NEW QUESTION 67
Refer to the exhibit.



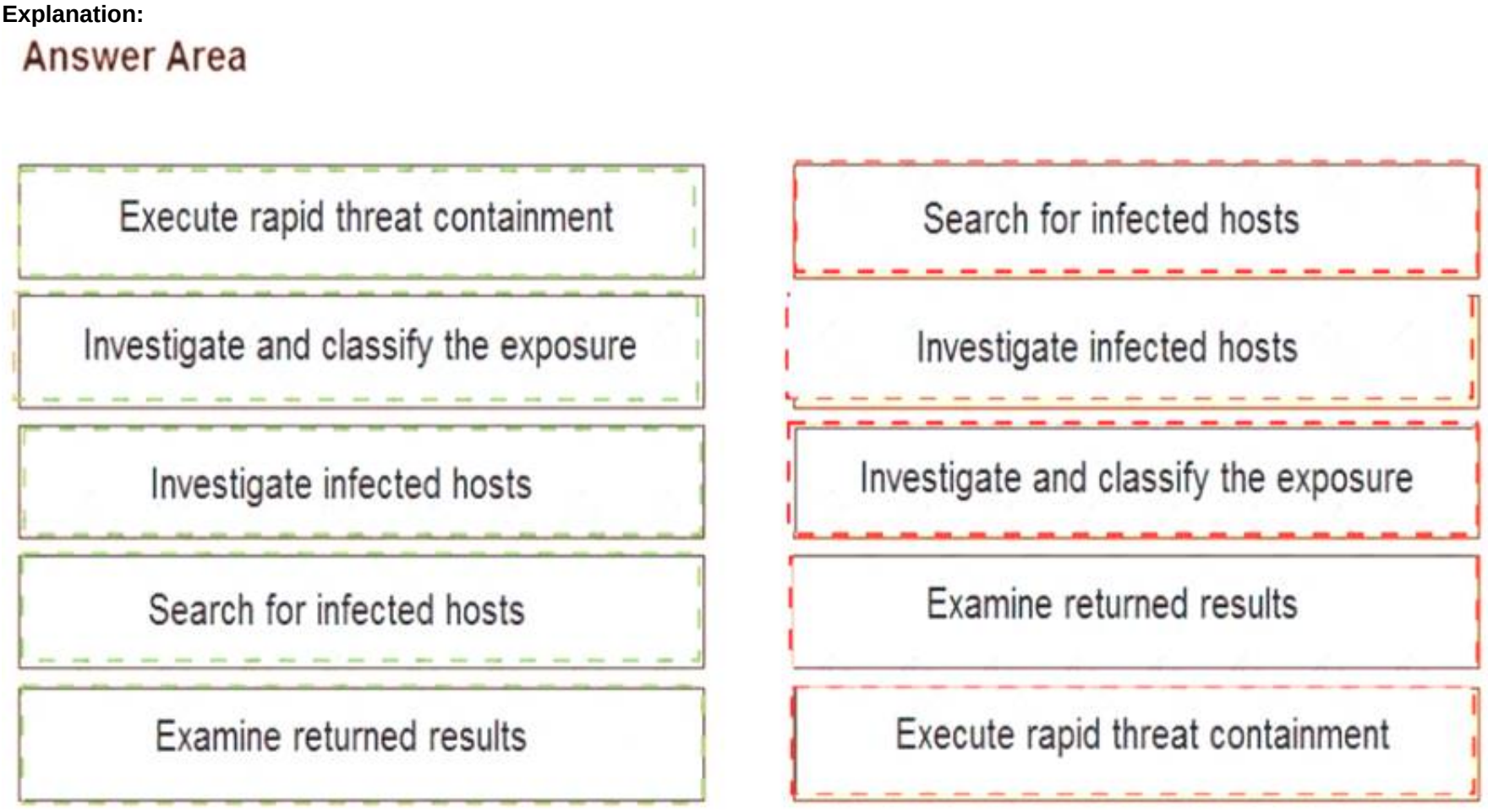
The Cisco Secure Network Analytics (Stealthwatch) console alerted with “New Malware Server Discovered” and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 68
An engineer received an alert of a zero-day vulnerability affecting desktop phones through which an attacker sends a crafted packet to a device, resets the credentials, makes the device unavailable, and allows a default administrator account login. Which step should an engineer take after receiving this alert?

A. Initiate a triage meeting to acknowledge the vulnerability and its potential impact
B. Determine company usage of the affected products
C. Search for a patch to install from the vendor
D. Implement restrictions within the VoIP VLANS

Answer: C

NEW QUESTION 71
A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

A. accessing the Active Directory server
B. accessing the server with financial data
C. accessing multiple servers
D. downloading more than 10 files

Answer: C

NEW QUESTION 75
Refer to the exhibit.

```
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
```

Where does it signify that a page will be stopped from loading when a scripting attack is detected?

A. x-frame-options
B. x-content-type-options
C. x-xss-protection
D. x-test-debug

Answer: C

NEW QUESTION 77
An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to "output alert_syslog: output log"
B. Modify the output module rule to "output alert_quick: output filename"
C. Modify the alert rule to "output alert_syslog: output header"
D. Modify the output module rule to "output alert_fast: output filename"

Answer: A

NEW QUESTION 81
A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

A. Run the sudo sysdiagnose command
B. Run the sh command
C. Run the w command
D. Run the who command

Answer: A

NEW QUESTION 86
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

350-201 Practice Exam Features:

* 350-201 Questions and Answers Updated Frequently

* 350-201 Practice Questions Verified by Expert Senior Certified Staff

* 350-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year