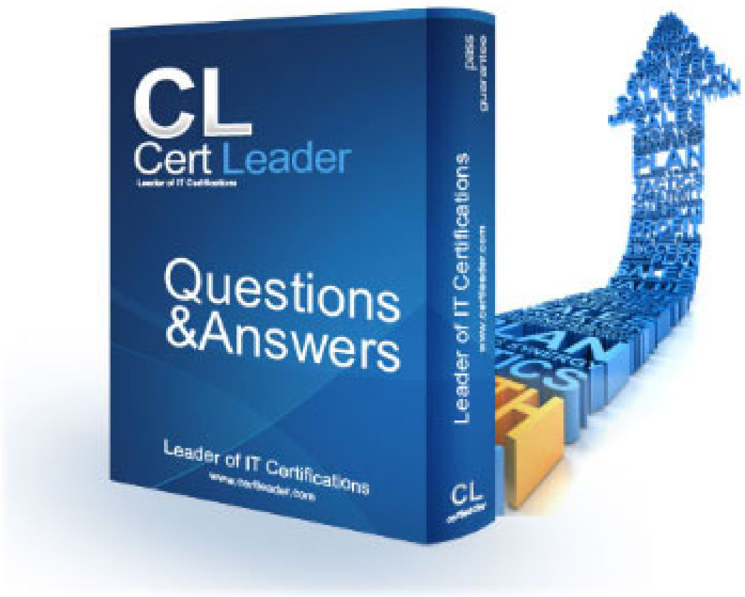
350-201 Dumps

Performing CyberOps Using Core Security Technologies (CBRCOR)

https://www.certleader.com/350-201-dumps.html



NEW QUESTION 1
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

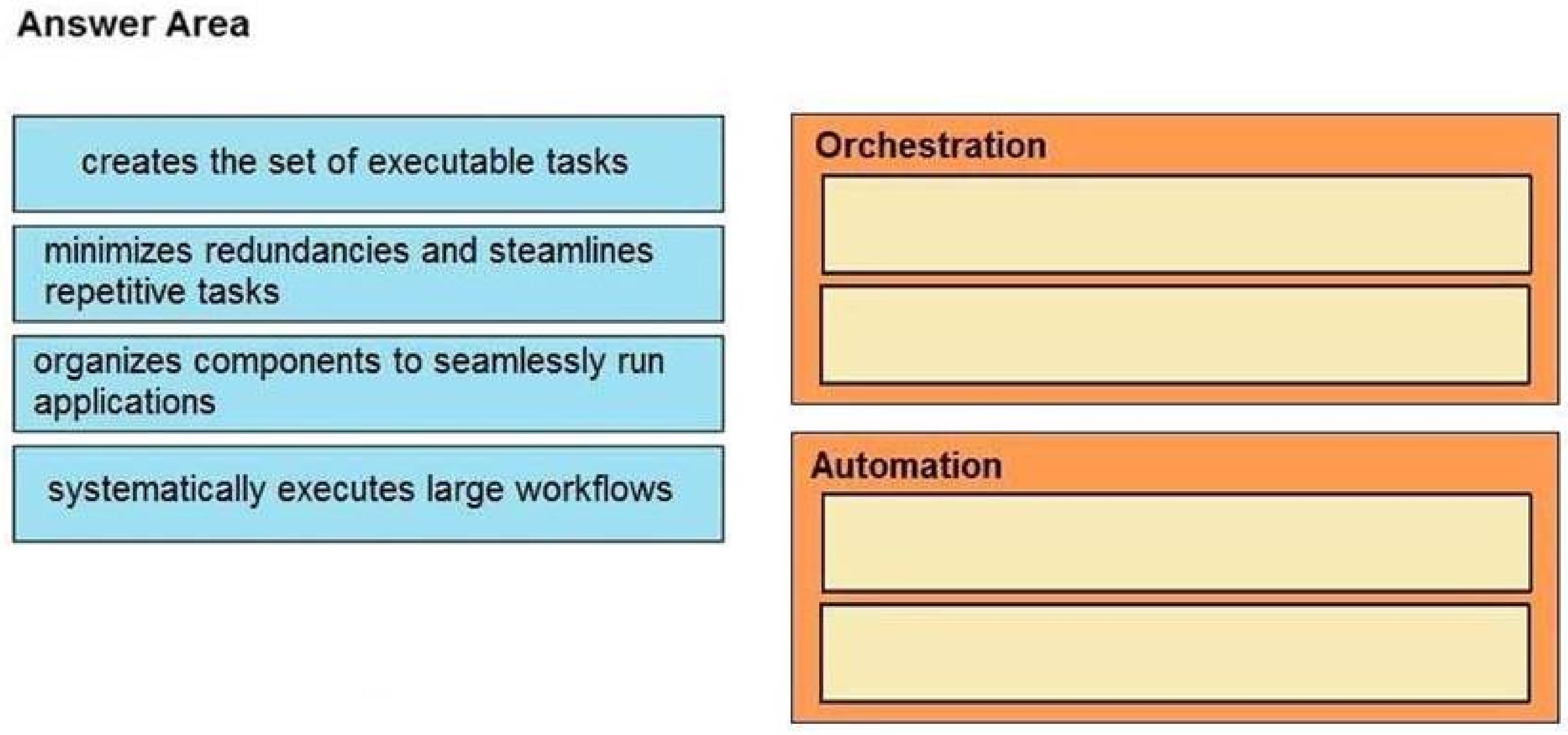
Answer: C

NEW QUESTION 2
An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering
B. data regression
C. data ingestion
D. data obfuscation

Answer: A

NEW QUESTION 3
Drag and drop the function on the left onto the mechanism on the right.



Answer Area

creates the set of executable tasks

minimizes redundancies and steamlines repetitive tasks

organizes components to seamlessly run applications

systematically executes large workflows

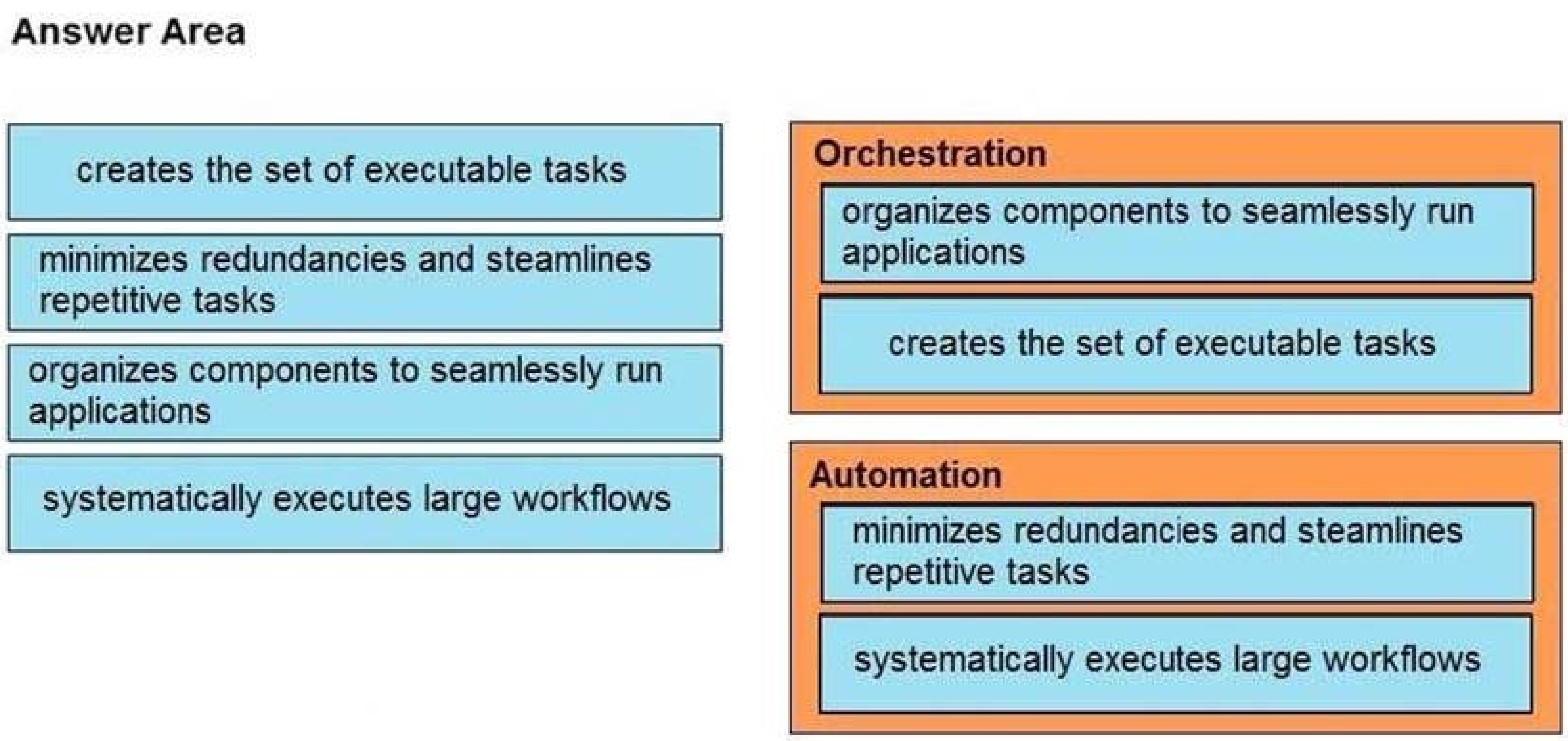
Orchestration

Automation

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

creates the set of executable tasks

minimizes redundancies and steamlines repetitive tasks

organizes components to seamlessly run applications

systematically executes large workflows

Orchestration

organizes components to seamlessly run applications

creates the set of executable tasks

Automation

minimizes redundancies and steamlines repetitive tasks

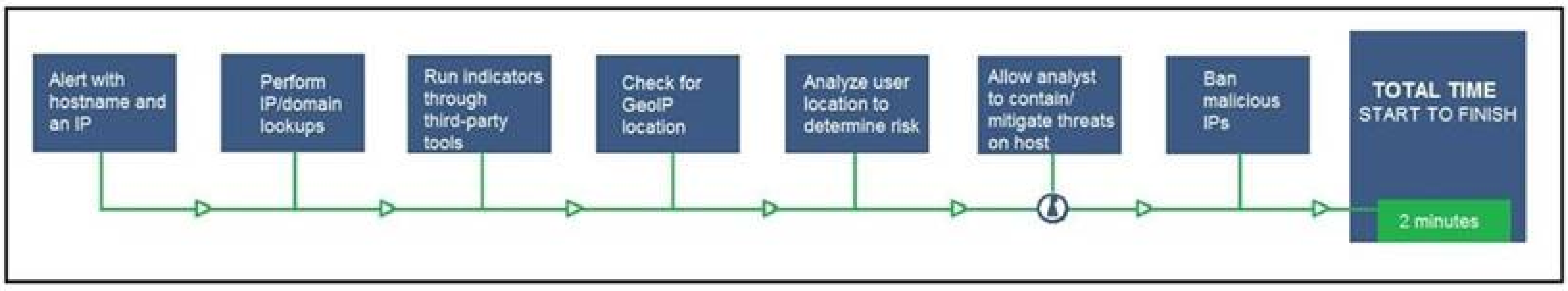
systematically executes large workflows

NEW QUESTION 4
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.

Answer: C

NEW QUESTION 5
Refer to the exhibit.


Alert with hostname and an IP
Perform IP/domain lookups
Run indicators through third-party tools
Check for GeoIP location
Analyze user location to determine risk
Allow analyst to contain/ mitigate threats on host
Ban malicious IPs
TOTAL TIME START TO FINISH
2 minutes

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 6
A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company’s infrastructure. Which steps should an engineer take at the recovery stage?

A. Determine the systems involved and deploy available patches
B. Analyze event logs and restrict network access
C. Review access lists and require users to increase password complexity
D. Identify the attack vector and update the IDS signature list

Answer: B

NEW QUESTION 7
A company’s web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and

vulnerabilities. Which additional element is needed to calculate the risk?

A. assessment scope
B. event severity and likelihood
C. incident response playbook
D. risk model framework

Answer: D

NEW QUESTION 8
An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

A. diagnostic
B. qualitative
C. predictive
D. statistical

Answer: C

NEW QUESTION 9
An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?

A. Investigate the vulnerability to prevent further spread
B. Acknowledge the vulnerabilities and document the risk
C. Apply vendor patches or available hot fixes
D. Isolate the assets affected in a separate network

Answer: D

NEW QUESTION 10
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

Answer: BE

NEW QUESTION 10
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 15
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 20
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

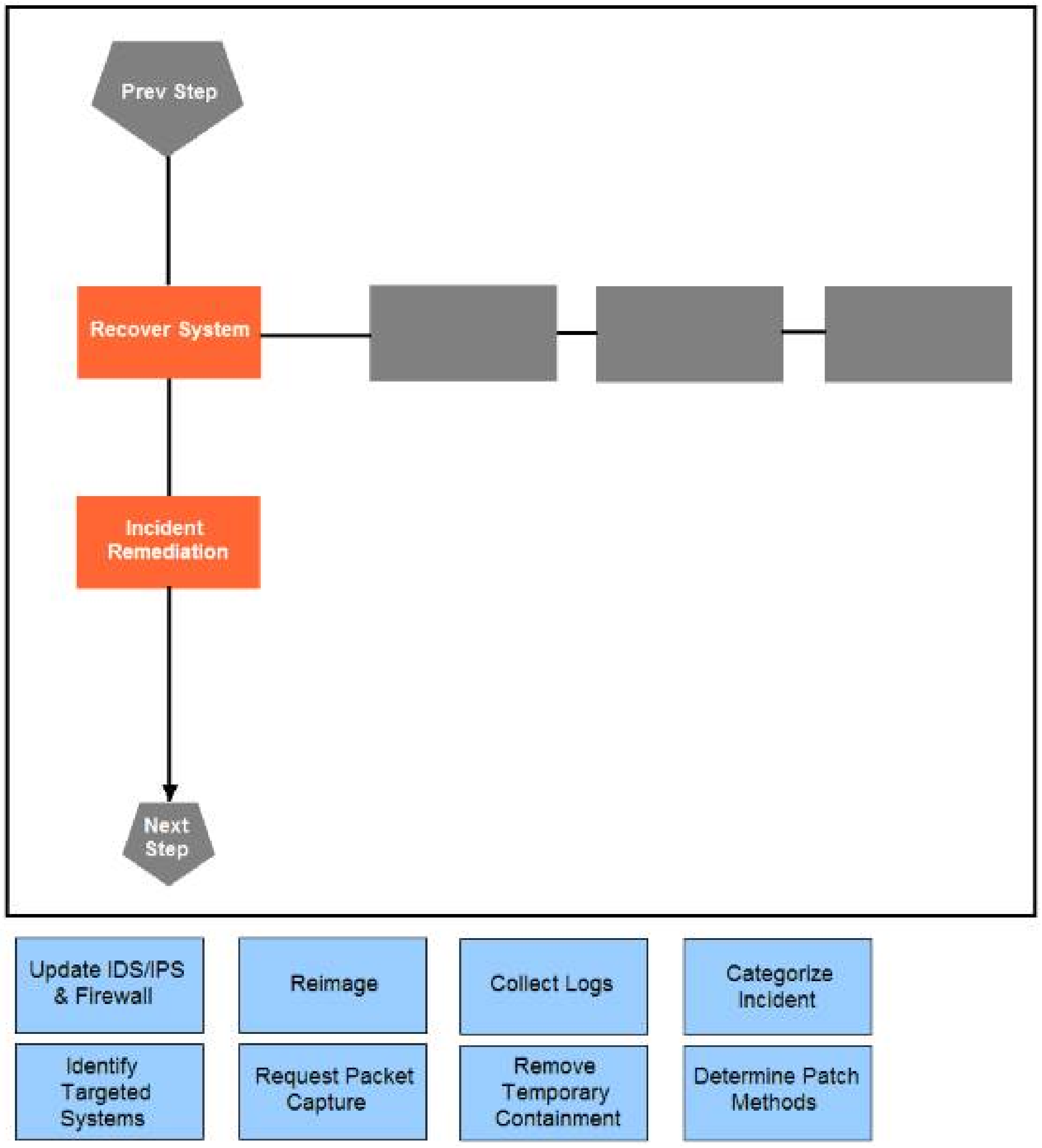
NEW QUESTION 24

A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets
B. Update software to patch third-party software
C. Validate CSRF by executing exploits within Metasploit
D. Fix applications according to the risk scores

Answer: D

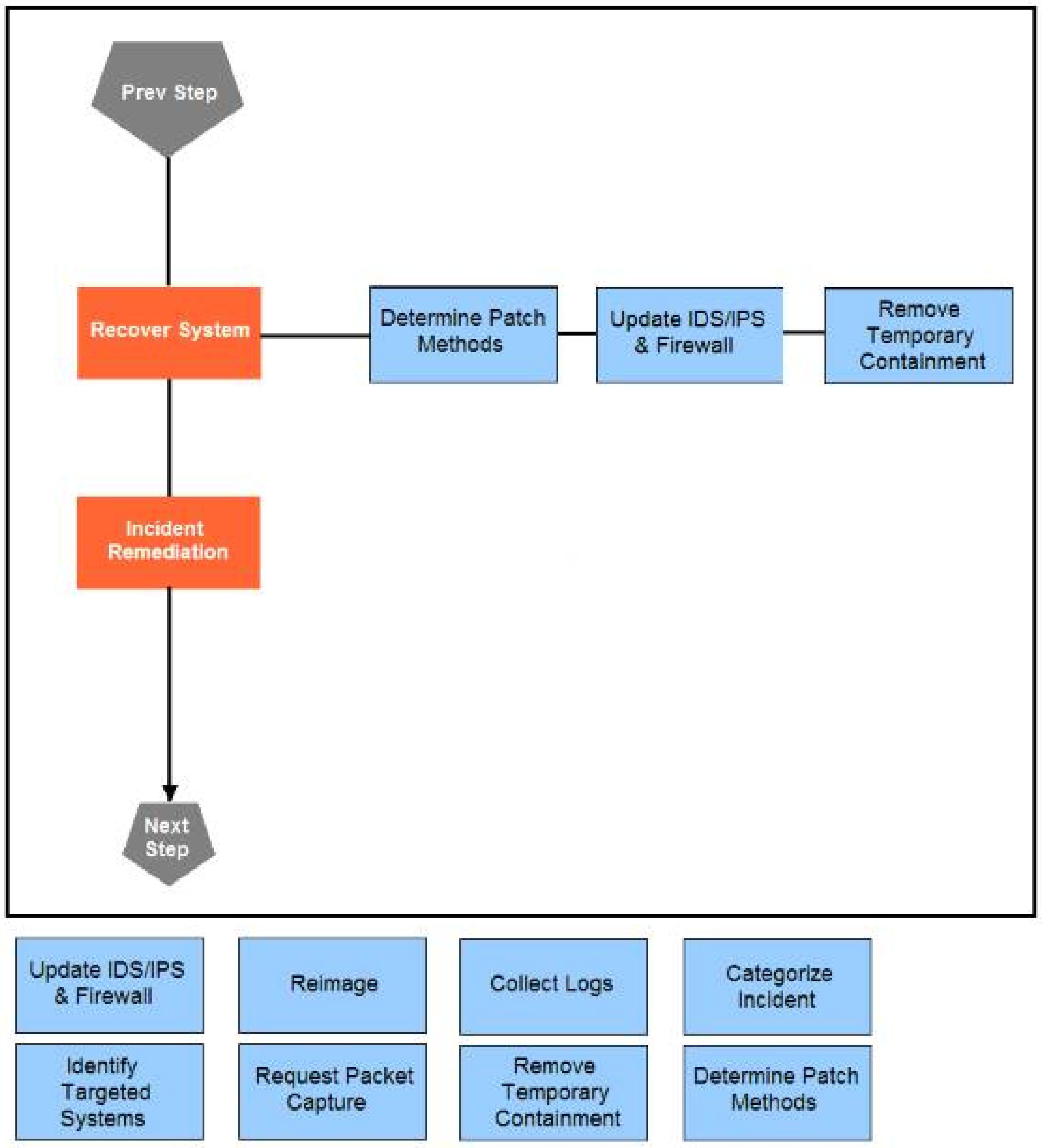
NEW QUESTION 26
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



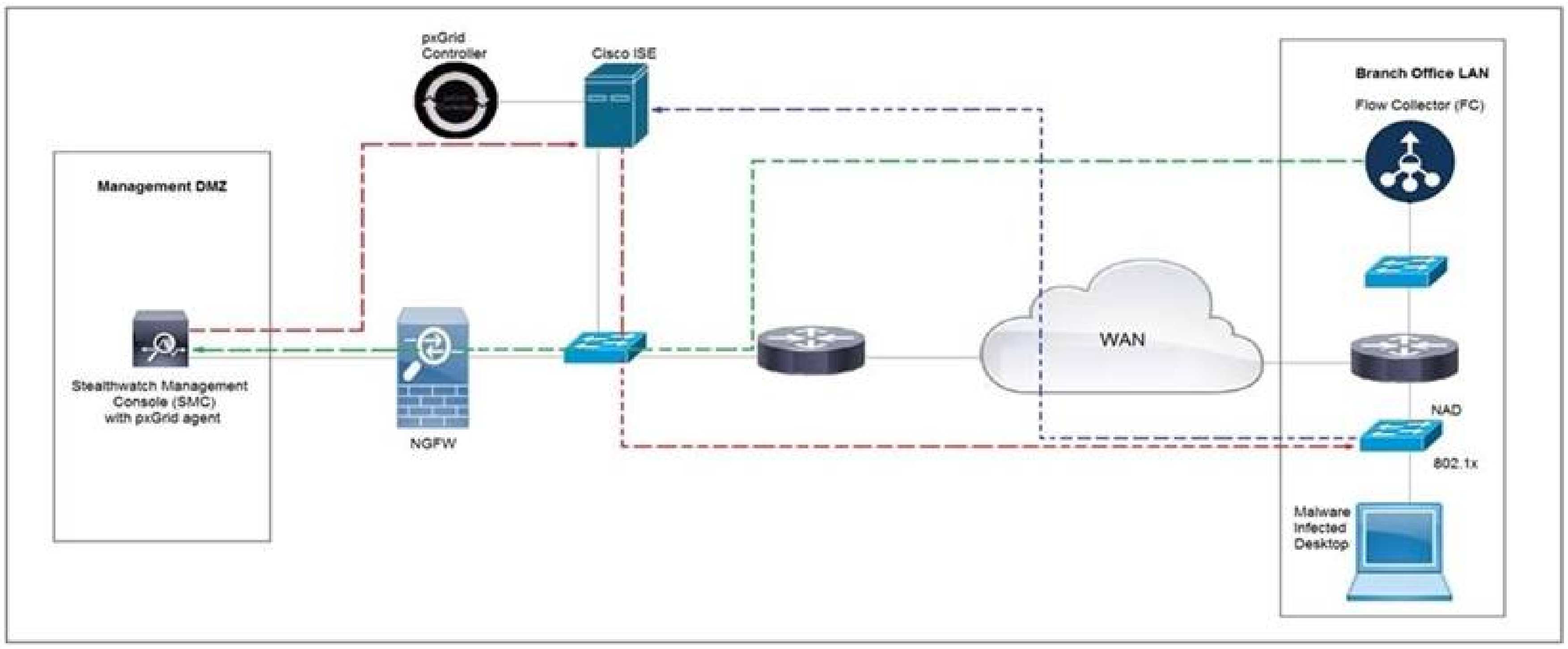
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 30
Refer to the exhibit.



Cisco 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 telemetry feeds were correlated with SMC to identify the malware?

A. NetFlow and event data
B. event data and syslog data
C. SNMP and syslog data
D. NetFlow and SNMP

Answer: B

NEW QUESTION 35
How does Wireshark decrypt TLS network traffic?

A. with a key log file using per-session secrets
B. using an RSA public key
C. by observing DH key exchange
D. by defining a user-specified decode-as

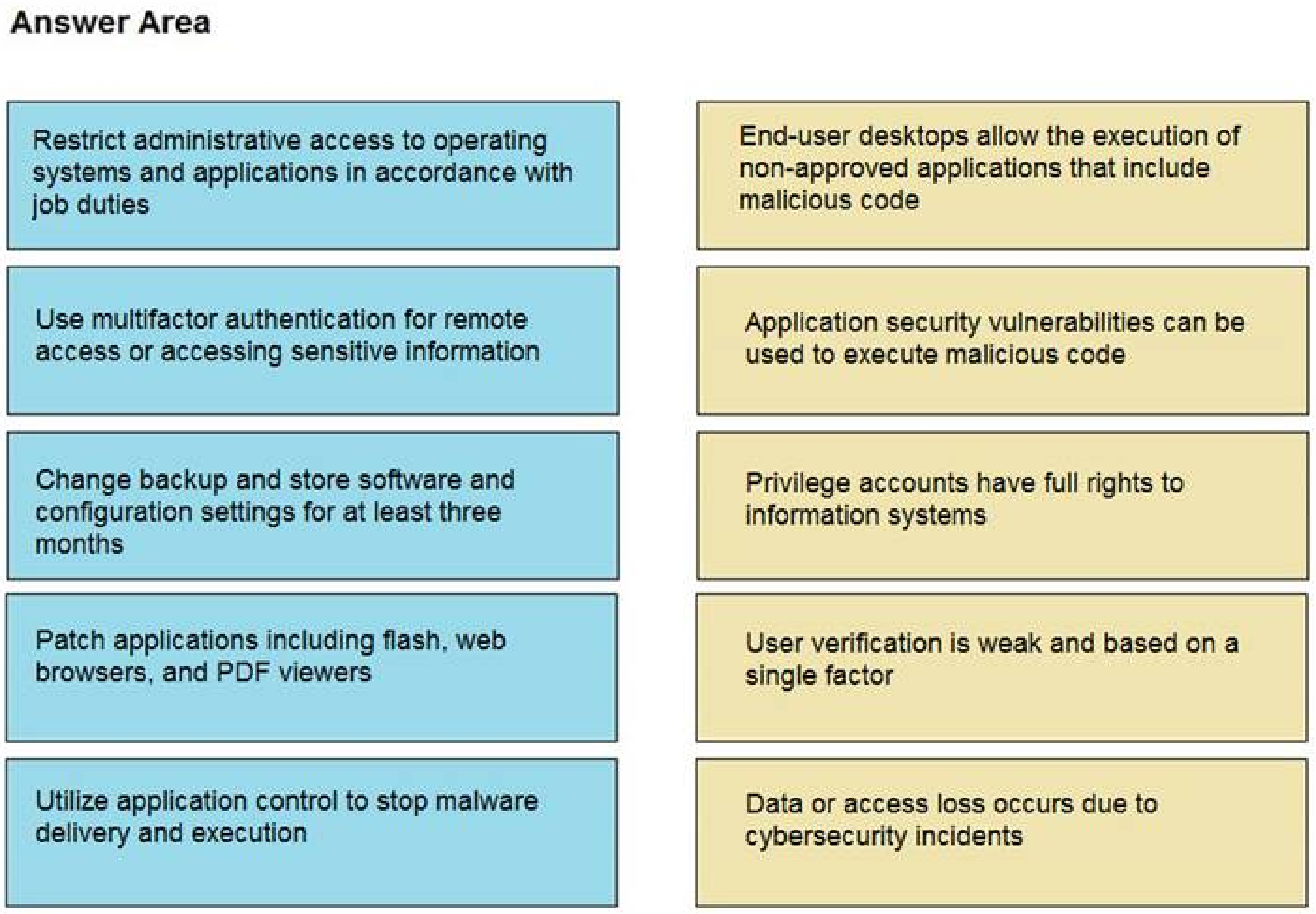
Answer: A

NEW QUESTION 39
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 44
Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.



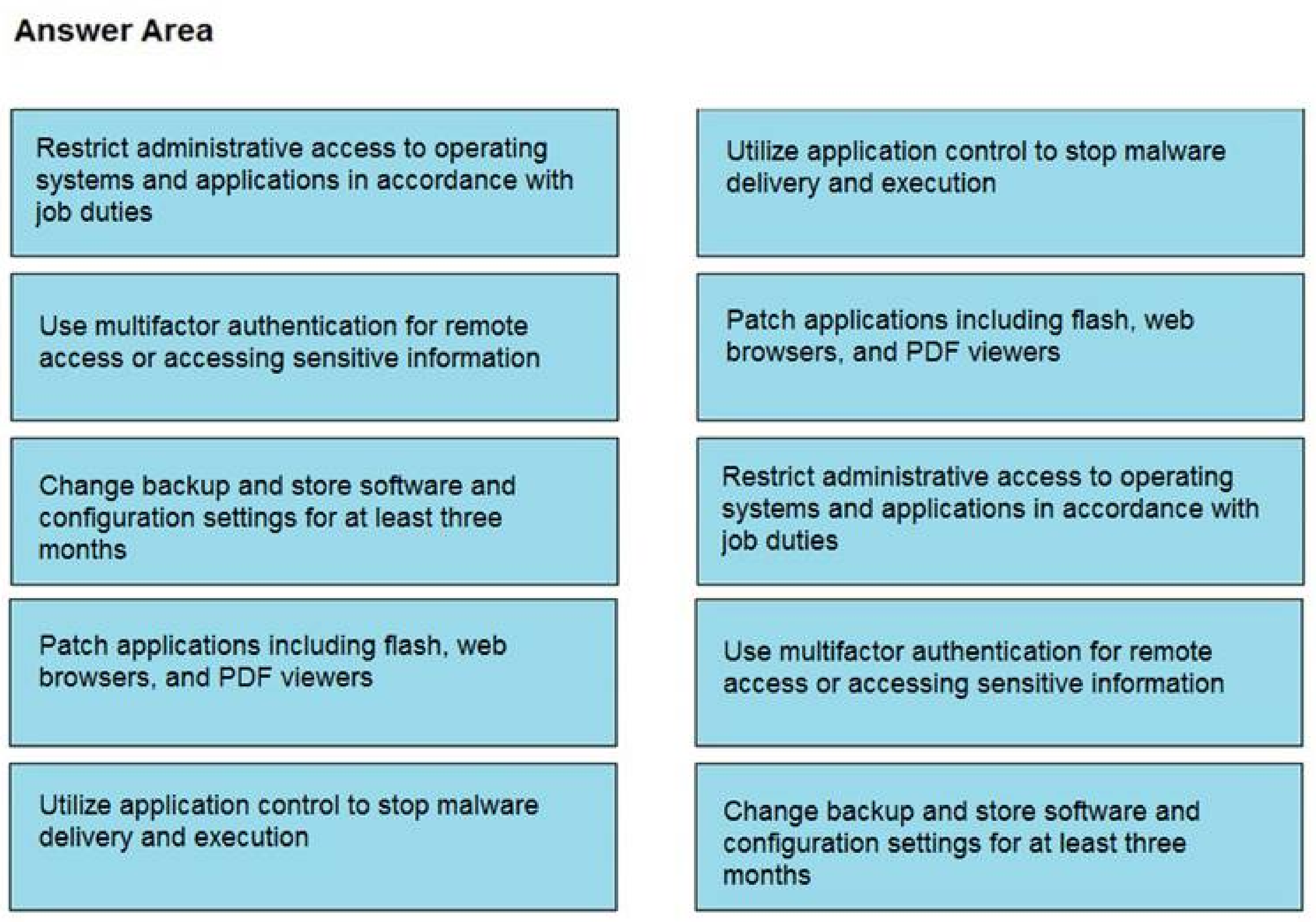
Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	End-user desktops allow the execution of non-approved applications that include malicious code
Use multifactor authentication for remote access or accessing sensitive information	Application security vulnerabilities can be used to execute malicious code
Change backup and store software and configuration settings for at least three months	Privilege accounts have full rights to information systems
Patch applications including flash, web browsers, and PDF viewers	User verification is weak and based on a single factor
Utilize application control to stop malware delivery and execution	Data or access loss occurs due to cybersecurity incidents

A. Mastered
B. Not Mastered

Answer: A

Explanation:

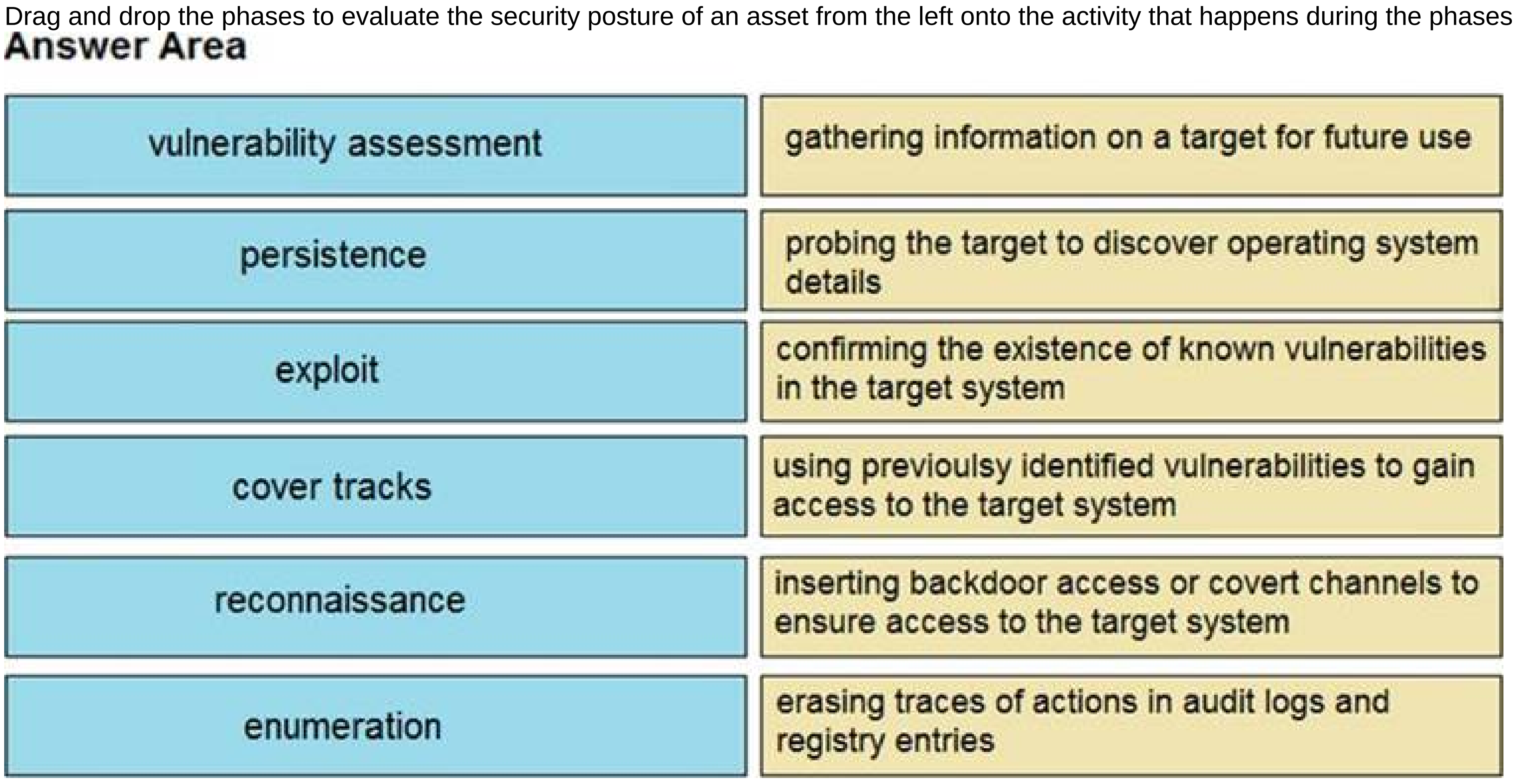


Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	Utilize application control to stop malware delivery and execution
Use multifactor authentication for remote access or accessing sensitive information	Patch applications including flash, web browsers, and PDF viewers
Change backup and store software and configuration settings for at least three months	Restrict administrative access to operating systems and applications in accordance with job duties
Patch applications including flash, web browsers, and PDF viewers	Use multifactor authentication for remote access or accessing sensitive information
Utilize application control to stop malware delivery and execution	Change backup and store software and configuration settings for at least three months

NEW QUESTION 48

Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.



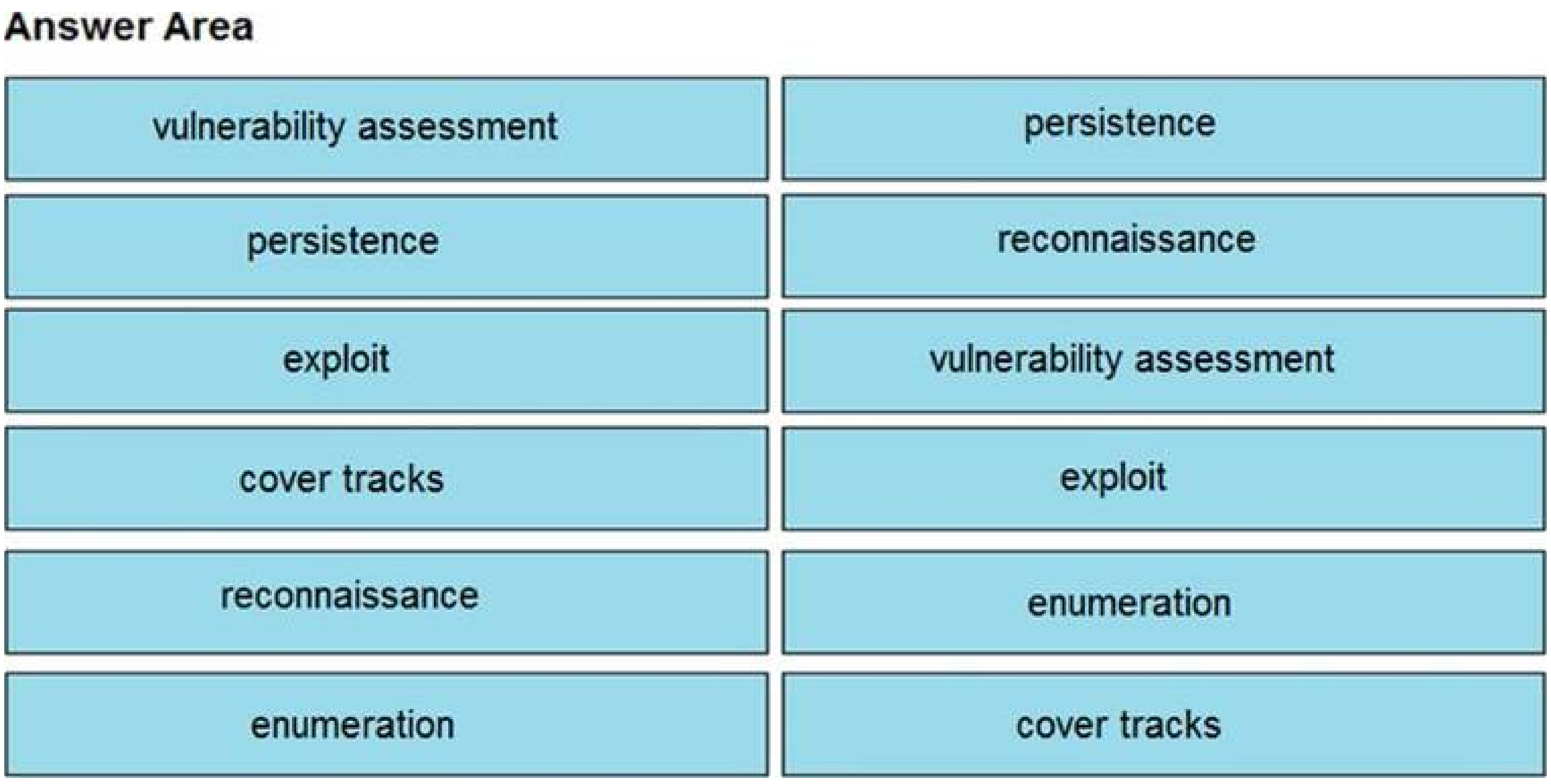
Answer Area

vulnerability assessment	gathering information on a target for future use
persistence	probing the target to discover operating system details
exploit	confirming the existence of known vulnerabilities in the target system
cover tracks	using previoulsy identified vulnerabilities to gain access to the target system
reconnaissance	inserting backdoor access or covert channels to ensure access to the target system
enumeration	erasing traces of actions in audit logs and registry entries

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

vulnerability assessment	persistence
persistence	reconnaissance
exploit	vulnerability assessment
cover tracks	exploit
reconnaissance	enumeration
enumeration	cover tracks

NEW QUESTION 53
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

Answer: B

NEW QUESTION 58
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

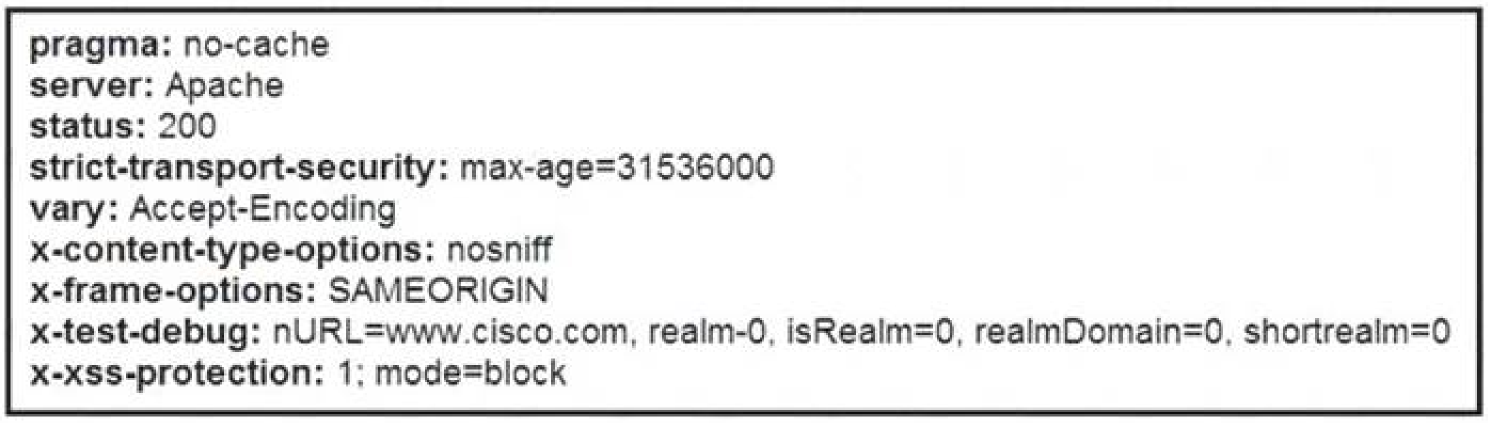
Answer: A

NEW QUESTION 59
A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user's working hours, what must the analyst do next to detect an abnormal behavior?

A. Create a rule triggered by 3 failed VPN connection attempts in an 8-hour period
B. Create a rule triggered by 1 successful VPN connection from any nondestination country
C. Create a rule triggered by multiple successful VPN connections from the destination countries
D. Analyze the logs from all countries related to this user during the traveling period

Answer: D

NEW QUESTION 60
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 61
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

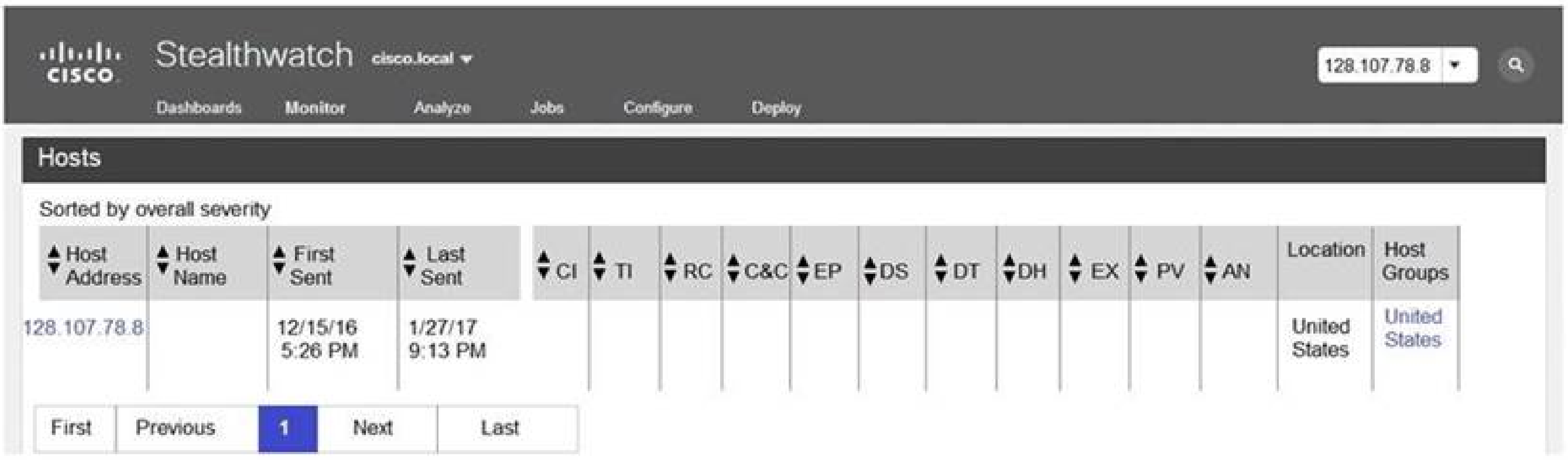
Answer: C

NEW QUESTION 63
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 68
Refer to the exhibit.

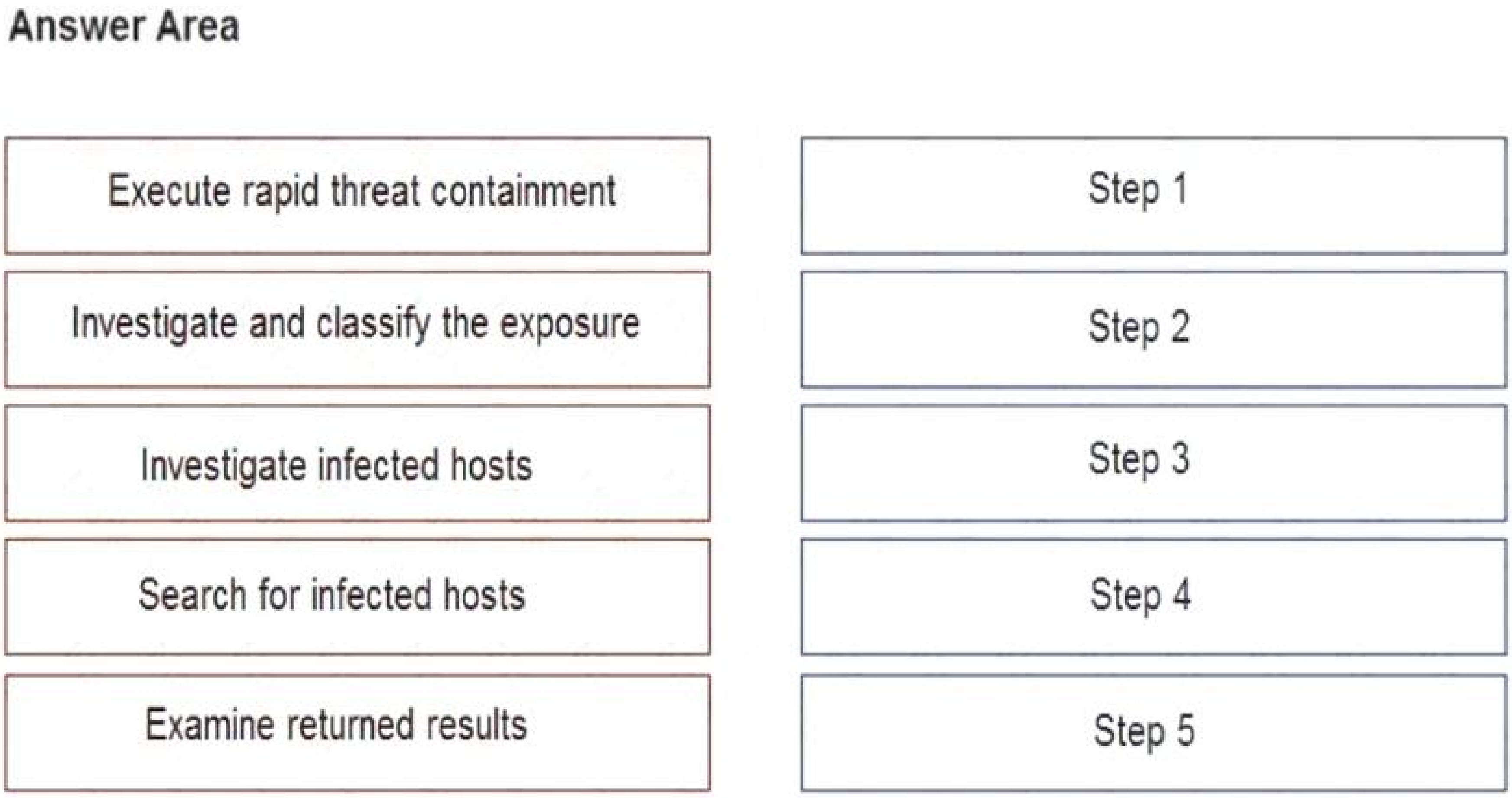


Hosts

Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States

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.


Answer Area

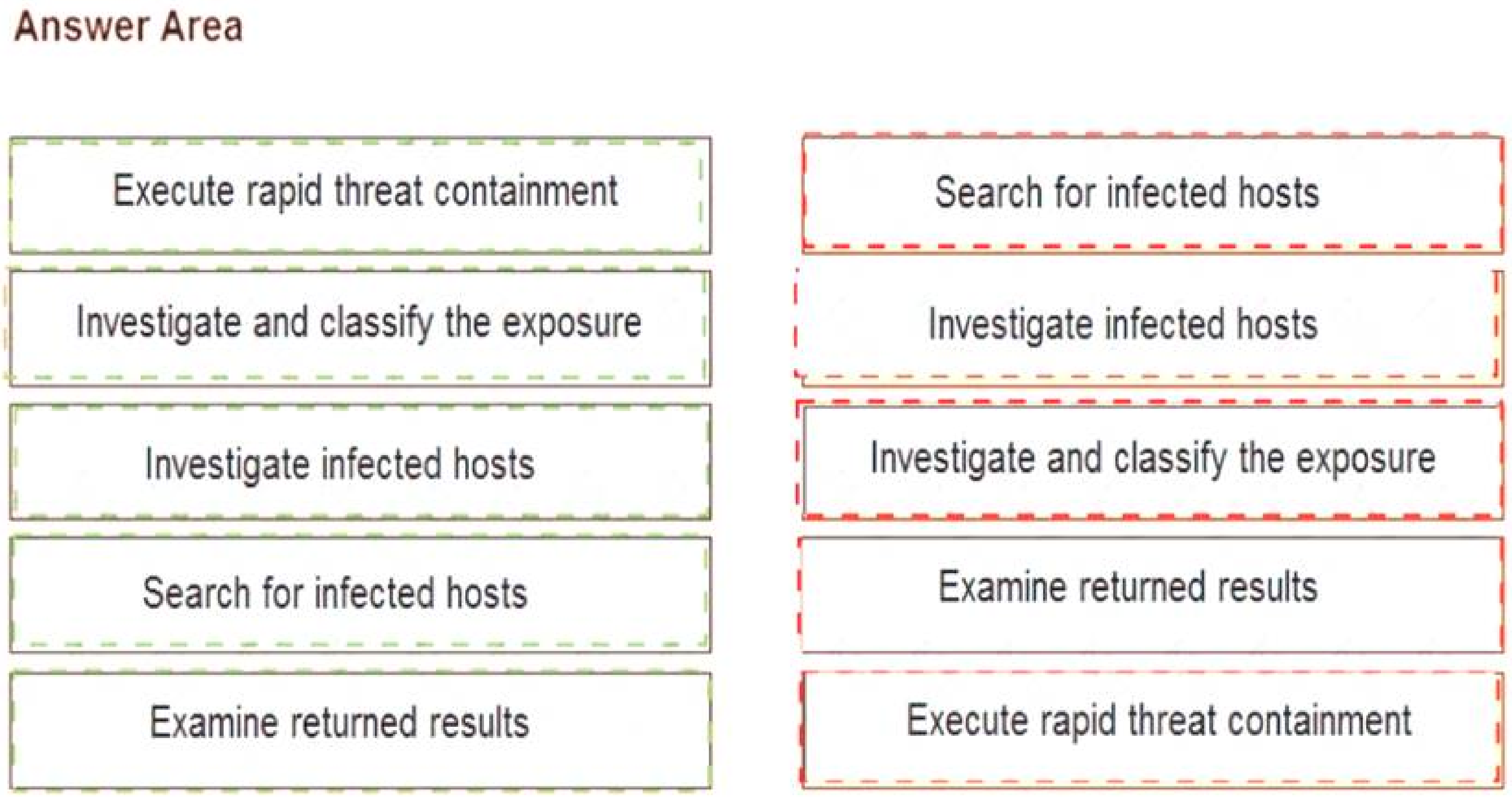
Execute rapid threat containment
Investigate and classify the exposure
Investigate infected hosts
Search for infected hosts
Examine returned results

Step 1
Step 2
Step 3
Step 4
Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Execute rapid threat containment	Search for infected hosts
Investigate and classify the exposure	Investigate infected hosts
Investigate infected hosts	Investigate and classify the exposure
Search for infected hosts	Examine returned results
Examine returned results	Execute rapid threat containment

NEW QUESTION 72

……