Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

A. chmod 666
B. chmod 774
C. chmod 775
D. chmod 777

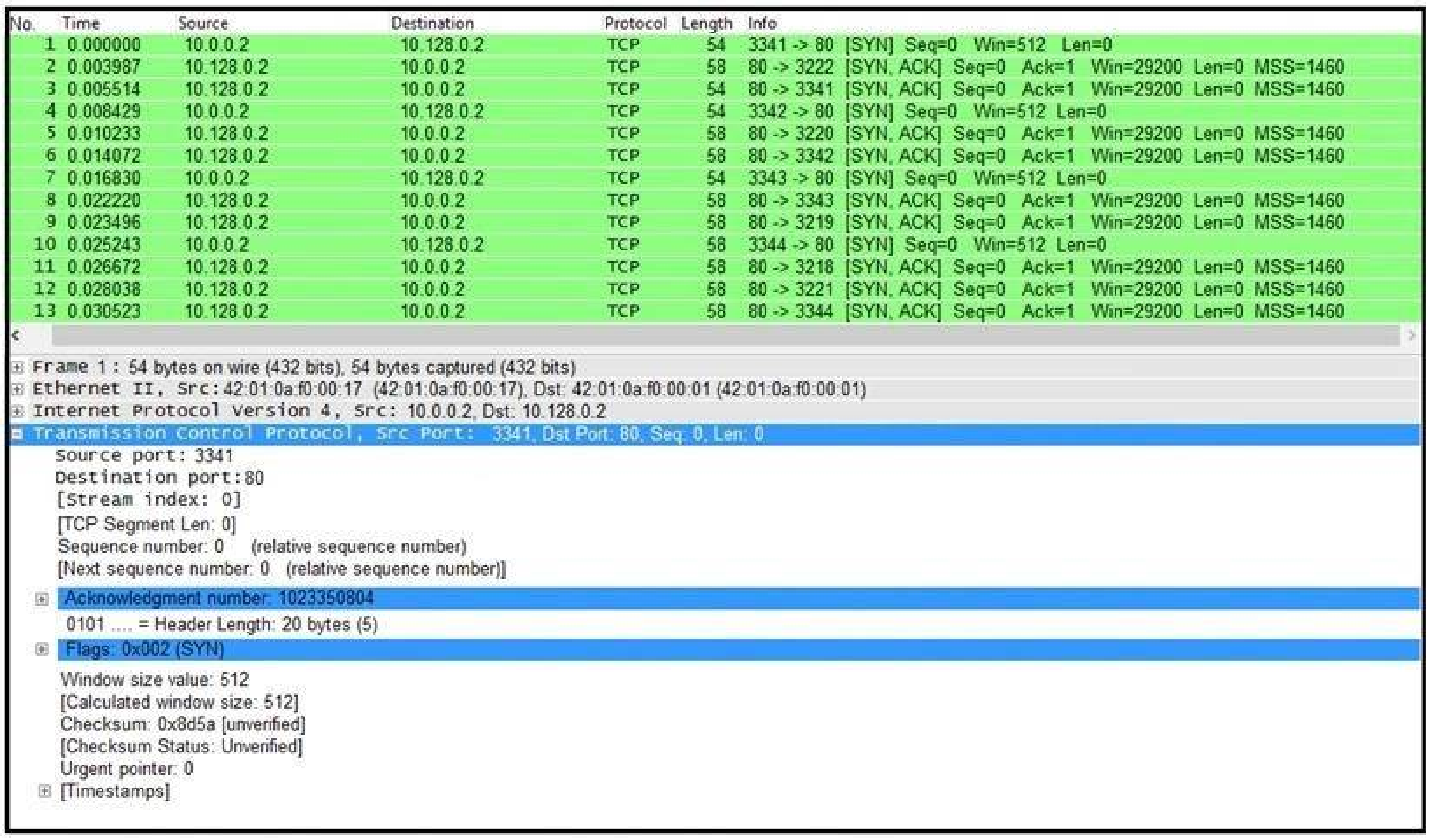
Answer: D

NEW QUESTION 2
The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

A. Determine the assets to which the attacker has access
B. Identify assets the attacker handled or acquired
C. Change access controls to high risk assets in the enterprise
D. Identify movement of the attacker in the enterprise

Answer: D

NEW QUESTION 3
Refer to the exhibit.



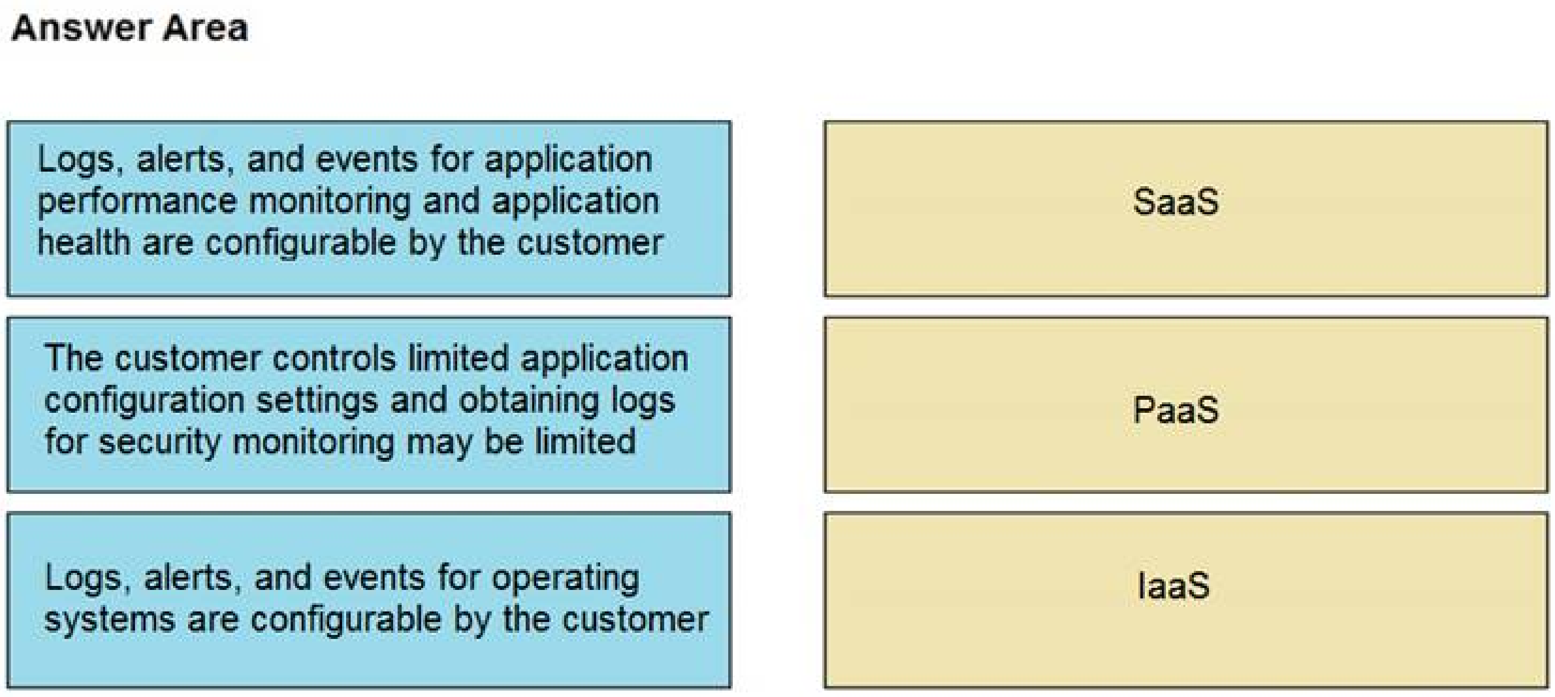
```
No.  Time      Source      Destination  Protocol Length Info
  1  0.000000  10.0.0.2    10.128.0.2   TCP      54     3341 -> 80 [SYN] Seq=0 Win=512 Len=0
  2  0.003987  10.128.0.2  10.0.0.2     TCP      58     80 -> 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  3  0.005514  10.128.0.2  10.0.0.2     TCP      54     80 -> 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  4  0.008429  10.0.0.2    10.128.0.2   TCP      54     3342 -> 80 [SYN] Seq=0 Win=512 Len=0
  5  0.010233  10.128.0.2  10.0.0.2     TCP      58     80 -> 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  6  0.014072  10.128.0.2  10.0.0.2     TCP      58     80 -> 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  7  0.016830  10.0.0.2    10.128.0.2   TCP      54     3343 -> 80 [SYN] Seq=0 Win=512 Len=0
  8  0.022220  10.128.0.2  10.0.0.2     TCP      58     80 -> 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  9  0.023496  10.128.0.2  10.0.0.2     TCP      58     80 -> 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 10  0.025243  10.0.0.2    10.128.0.2   TCP      58     3344 -> 80 [SYN] Seq=0 Win=512 Len=0
 11  0.026672  10.128.0.2  10.0.0.2     TCP      58     80 -> 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 12  0.028038  10.128.0.2  10.0.0.2     TCP      58     80 -> 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 13  0.030523  10.128.0.2  10.0.0.2     TCP      58     80 -> 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

⊞ Frame 1 : 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
⊞ Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2
⊟ Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
     Source port: 3341
     Destination port:80
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     [Next sequence number: 0   (relative sequence number)]
  ⊞  Acknowledgment number: 1023350804
      0101 .... = Header Length: 20 bytes (5)
  ⊞  Flags: 0x002 (SYN)
     Window size value: 512
     [Calculated window size: 512]
     Checksum: 0x8d5a [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
  ⊞  [Timestamps]
```

What is the threat in this Wireshark traffic capture?

A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
B. A flood of ACK packets coming from a single source IP to multiple destination IPs
C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs
D. A flood of SYN packets coming from a single source IP to a single destination IP

Answer: D

NEW QUESTION 4
Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.



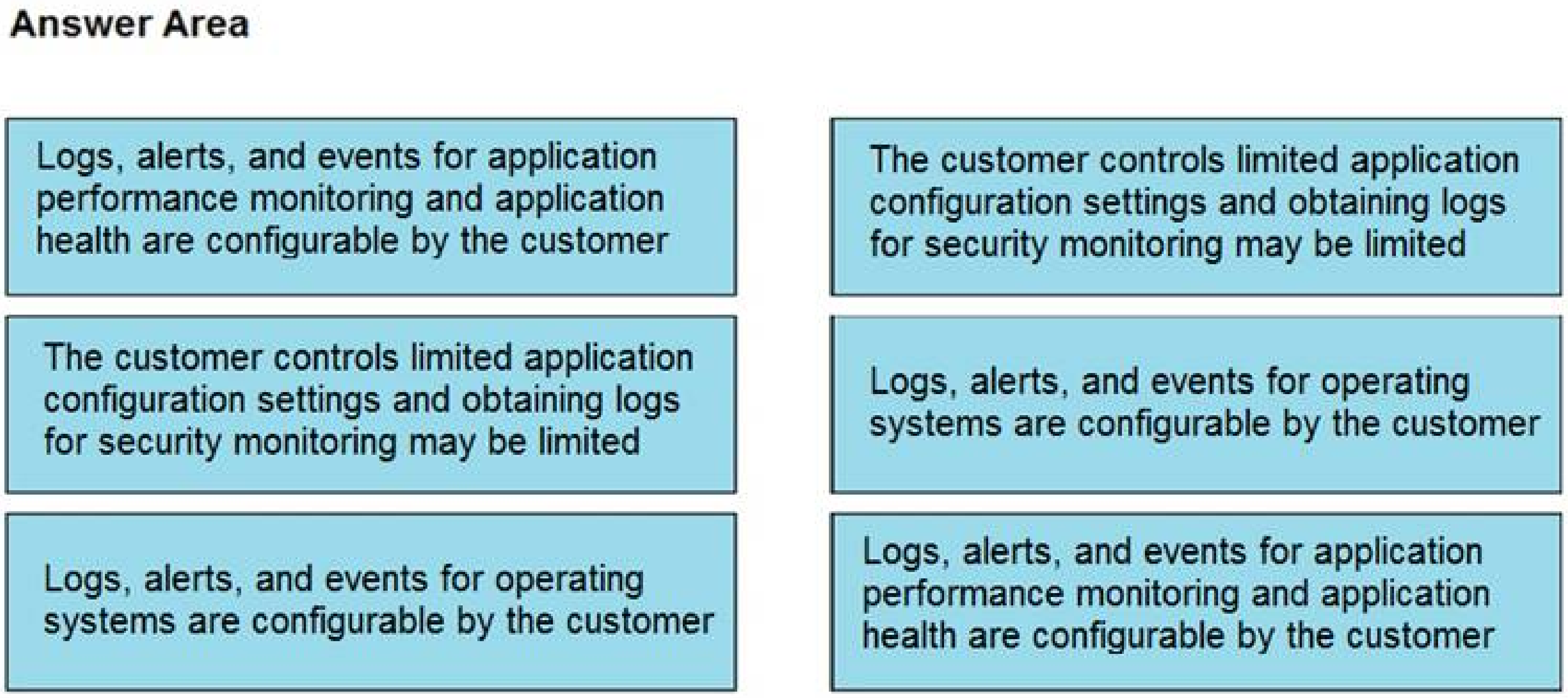
Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	SaaS
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	PaaS
Logs, alerts, and events for operating systems are configurable by the customer	IaaS

A. Mastered
B. Not Mastered

Answer: A

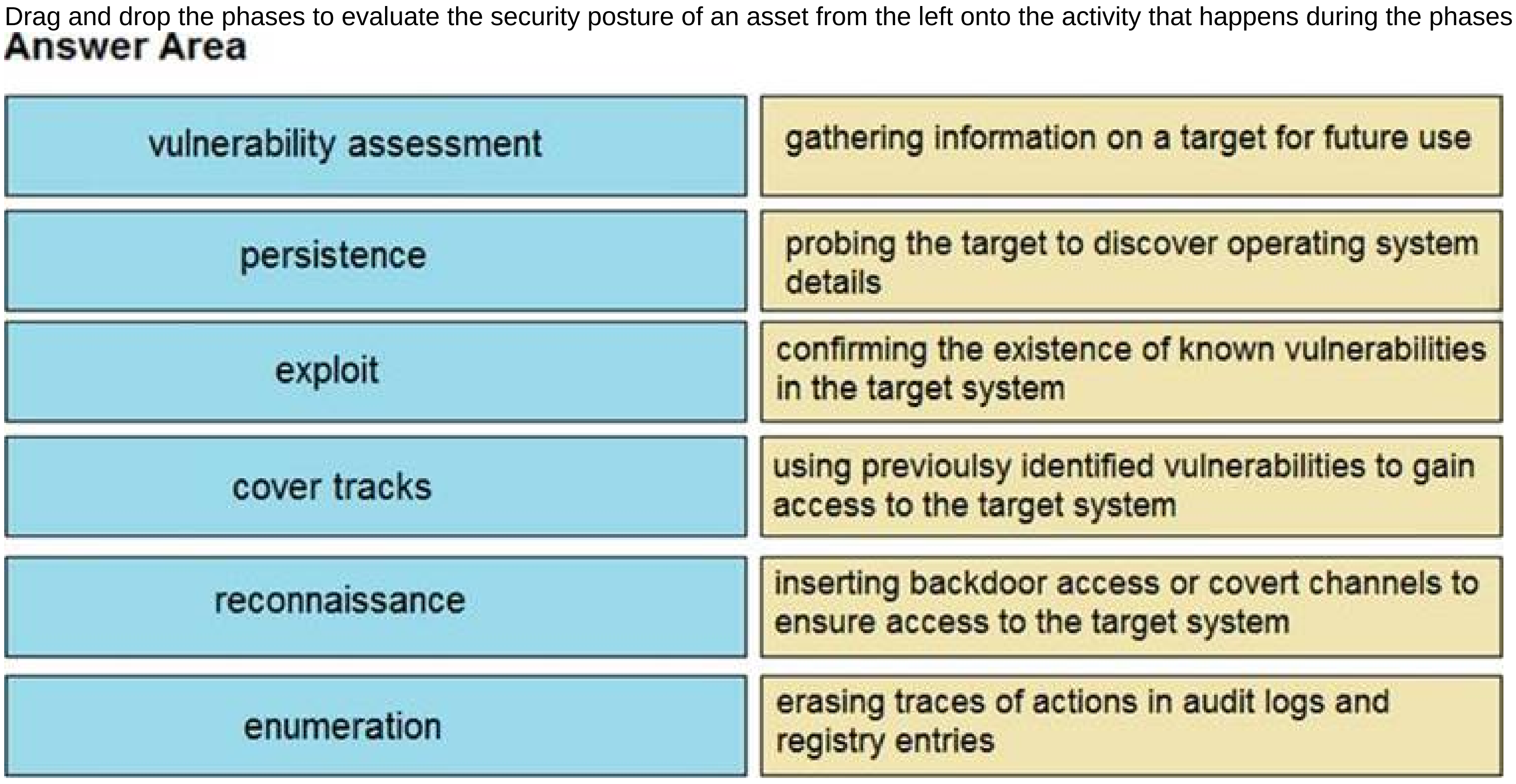
Explanation:



Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	Logs, alerts, and events for operating systems are configurable by the customer
Logs, alerts, and events for operating systems are configurable by the customer	Logs, alerts, and events for application performance monitoring and application health are configurable by the customer

NEW QUESTION 5
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.



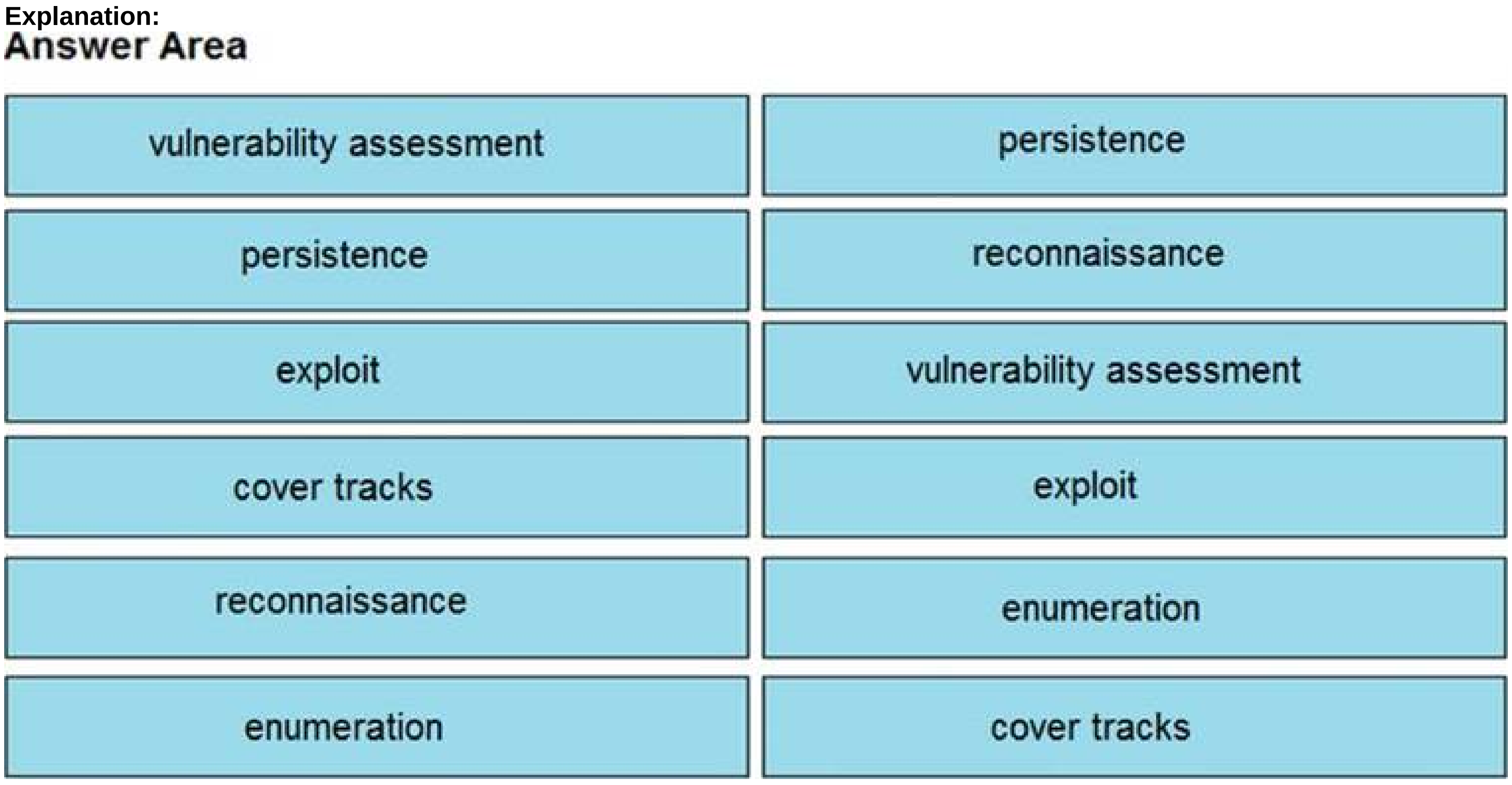
Answer Area

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:

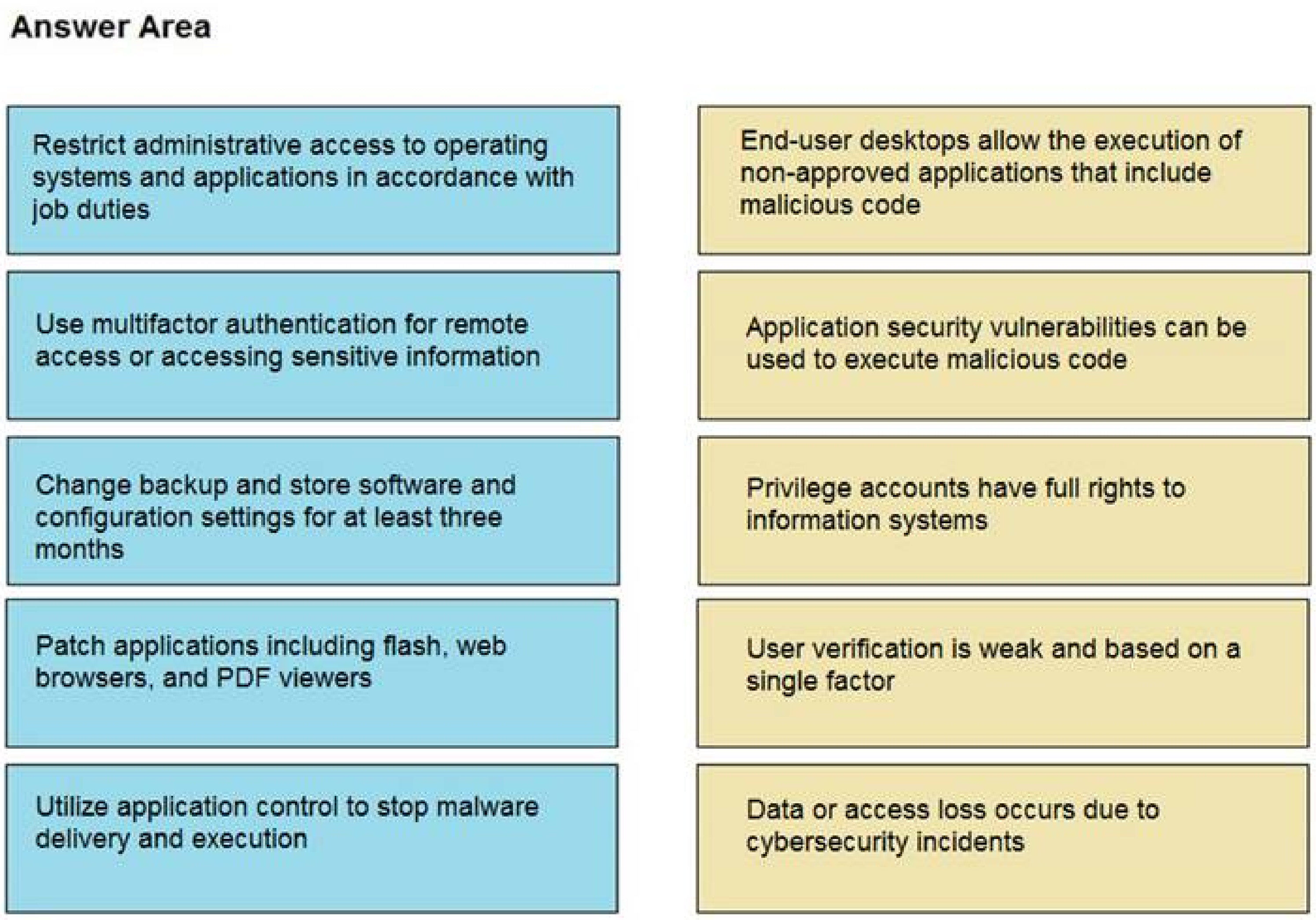


Answer Area

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

NEW QUESTION 6

Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.



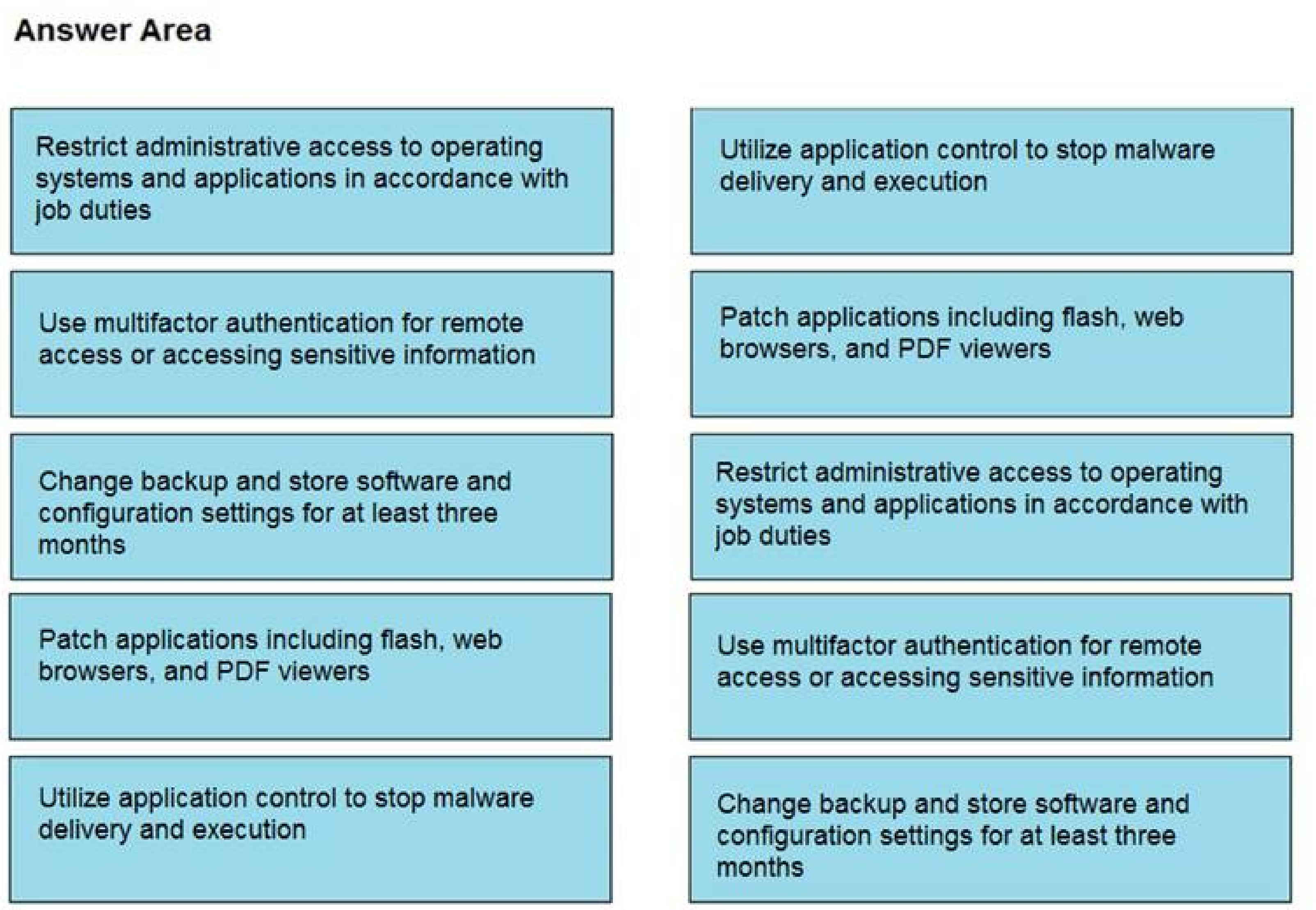
Answer Area

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 7
Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system's startup folder. It appears that the shortcuts redirect users to malicious URLs. What is the next step the engineer should take to investigate this case?

A. Remove the shortcut files
B. Check the audit logs
C. Identify affected systems
D. Investigate the malicious URLs

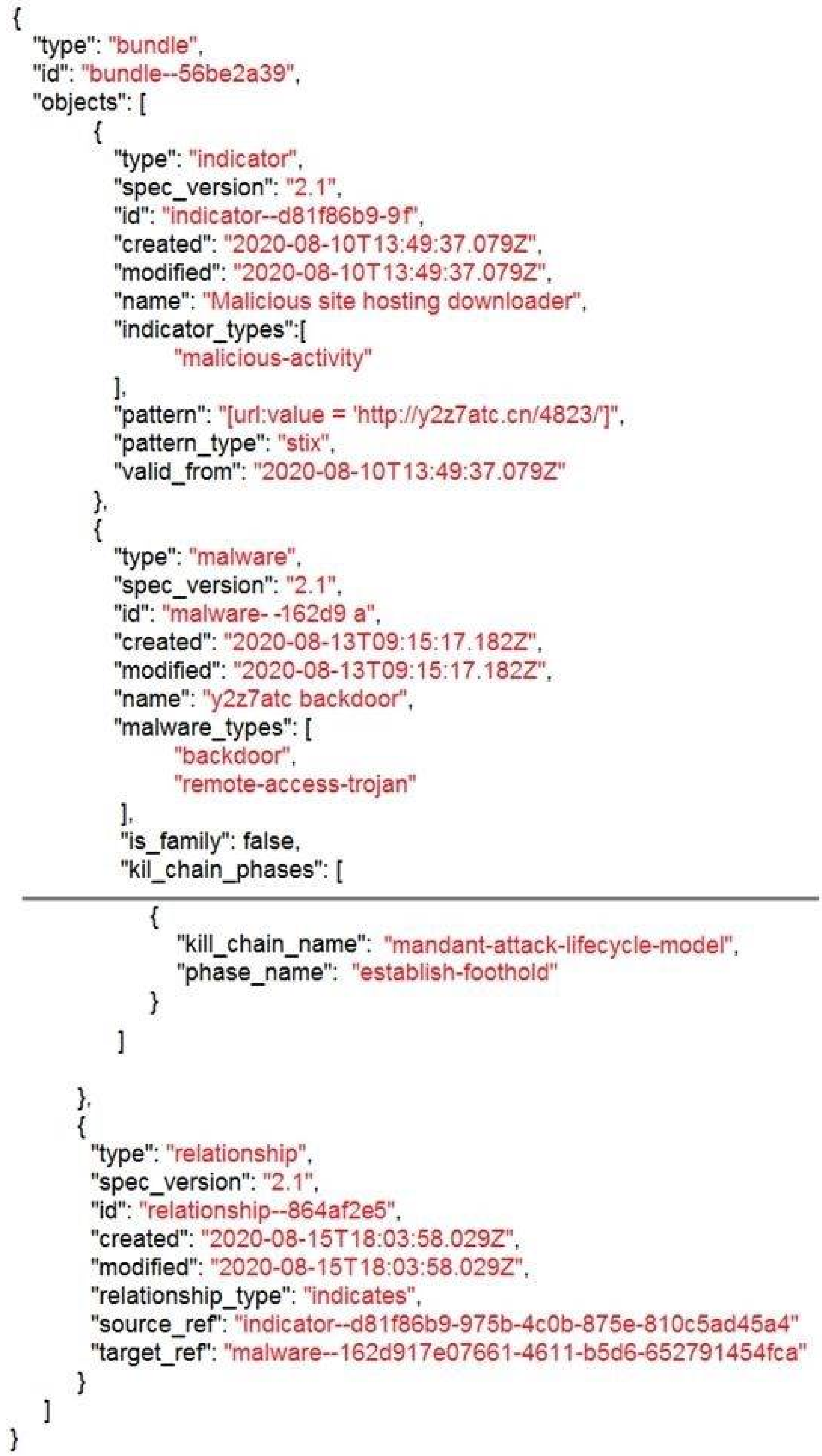
Answer: C

NEW QUESTION 8
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
B. Ask the company to execute the payload for real time analysis
C. Investigate further in open source repositories using YARA to find matches
D. Obtain a copy of the file for detonation in a sandbox

Answer: D

NEW QUESTION 9
Refer to the exhibit.



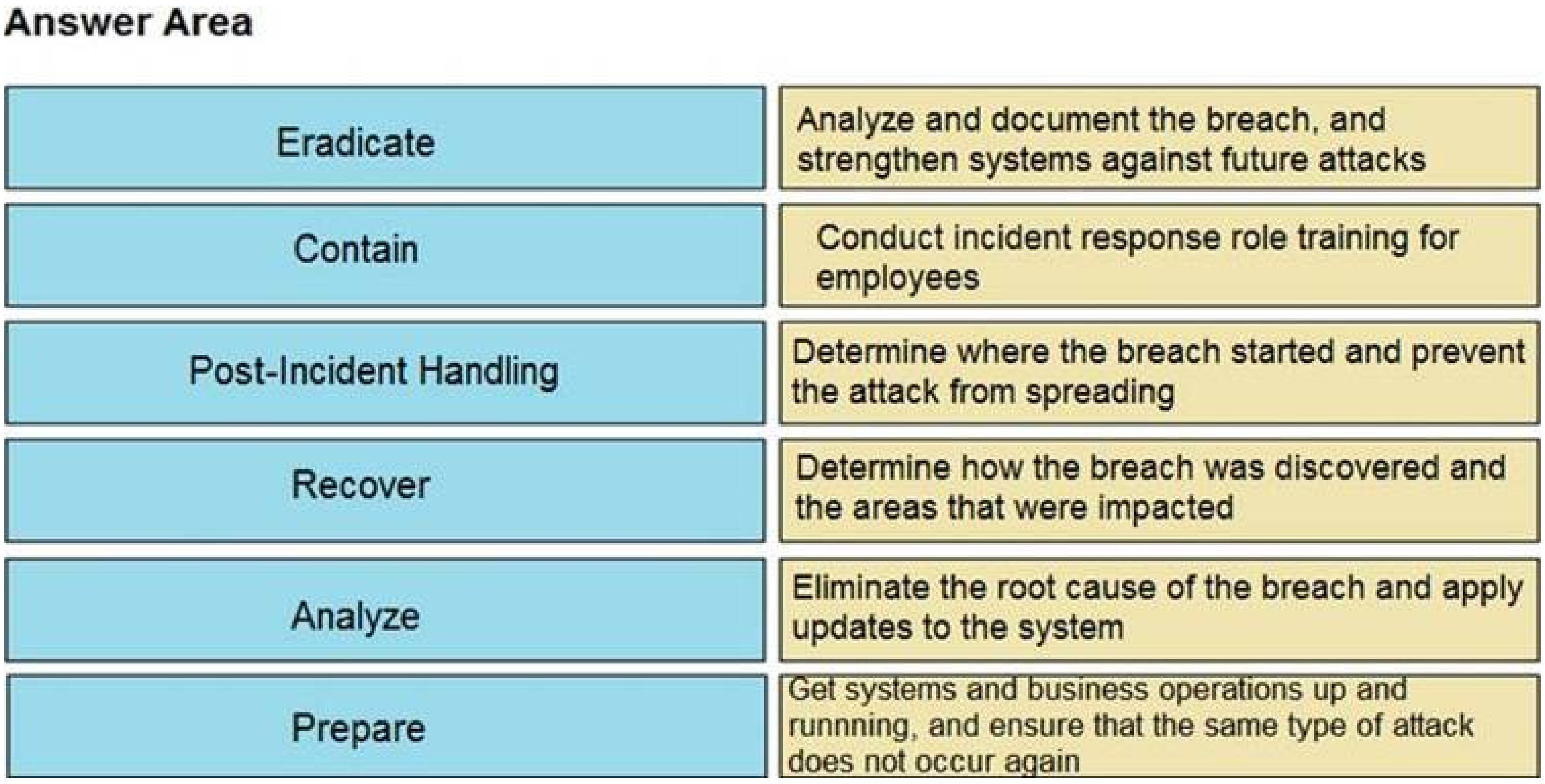
```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
        {
          "type": "indicator",
          "spec_version": "2.1",
          "id": "indicator--d81f86b9-9f",
          "created": "2020-08-10T13:49:37.079Z",
          "modified": "2020-08-10T13:49:37.079Z",
          "name": "Malicious site hosting downloader",
          "indicator_types":[
                "malicious-activity"
          ],
          "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
          "pattern_type": "stix",
          "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
          "type": "malware",
          "spec_version": "2.1",
          "id": "malware- -162d9 a",
          "created": "2020-08-13T09:15:17.182Z",
          "modified": "2020-08-13T09:15:17.182Z",
          "name": "y2z7atc backdoor",
          "malware_types": [
                "backdoor",
                "remote-access-trojan"
           ],
           "is_family": false,
           "kil_chain_phases": [
              {
                "kill_chain_name":  "mandant-attack-lifecycle-model",
                "phase_name":  "establish-foothold"
              }
           ]

      },
      {
        "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--864af2e5",
        "created": "2020-08-15T18:03:58.029Z",
        "modified": "2020-08-15T18:03:58.029Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4",
        "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
      }
    ]
}
```

Which indicator of compromise is represented by this STIX?

A. website redirecting traffic to ransomware server
B. website hosting malware to download files
C. web server vulnerability exploited by malware
D. cross-site scripting vulnerability to backdoor server

Answer: C

NEW QUESTION 10
Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.



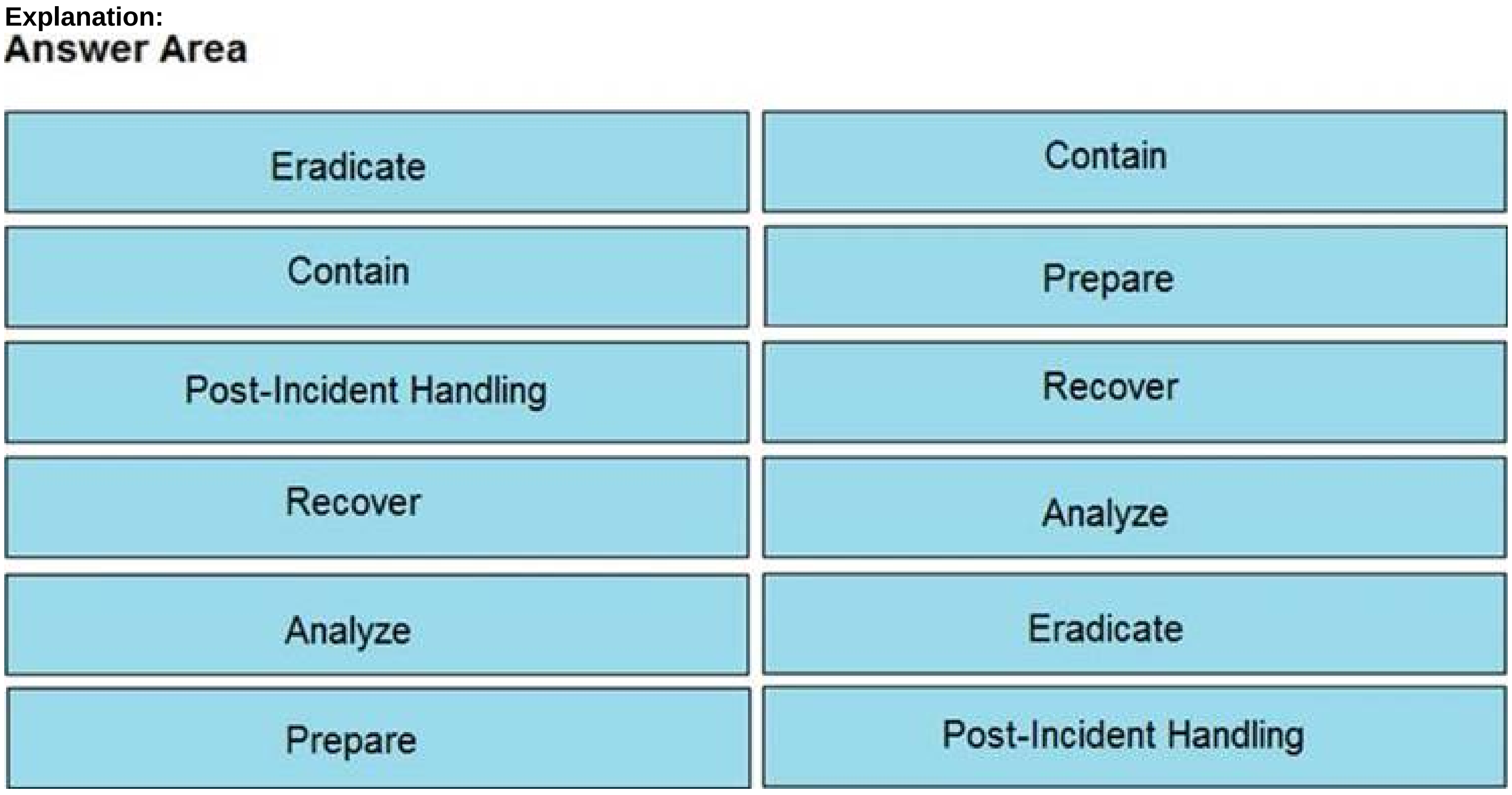
Answer Area

Eradicate	Analyze and document the breach, and strengthen systems against future attacks
Contain	Conduct incident response role training for employees
Post-Incident Handling	Determine where the breach started and prevent the attack from spreading
Recover	Determine how the breach was discovered and the areas that were impacted
Analyze	Eliminate the root cause of the breach and apply updates to the system
Prepare	Get systems and business operations up and runnning, and ensure that the same type of attack does not occur again

A. Mastered
B. Not Mastered

Answer: A

Explanation:

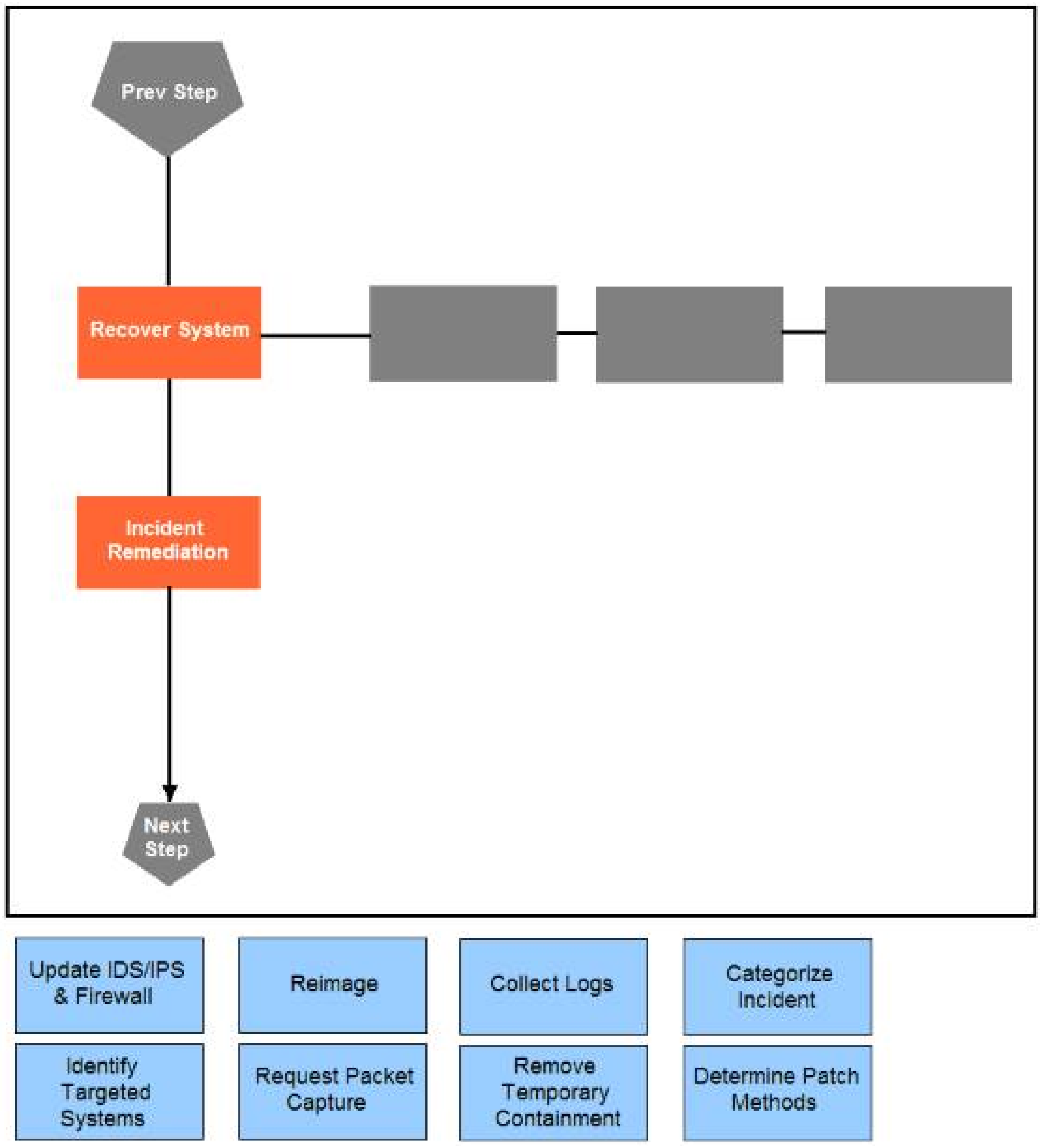


Answer Area

Eradicate	Contain
Contain	Prepare
Post-Incident Handling	Recover
Recover	Analyze
Analyze	Eradicate
Prepare	Post-Incident Handling

NEW QUESTION 10

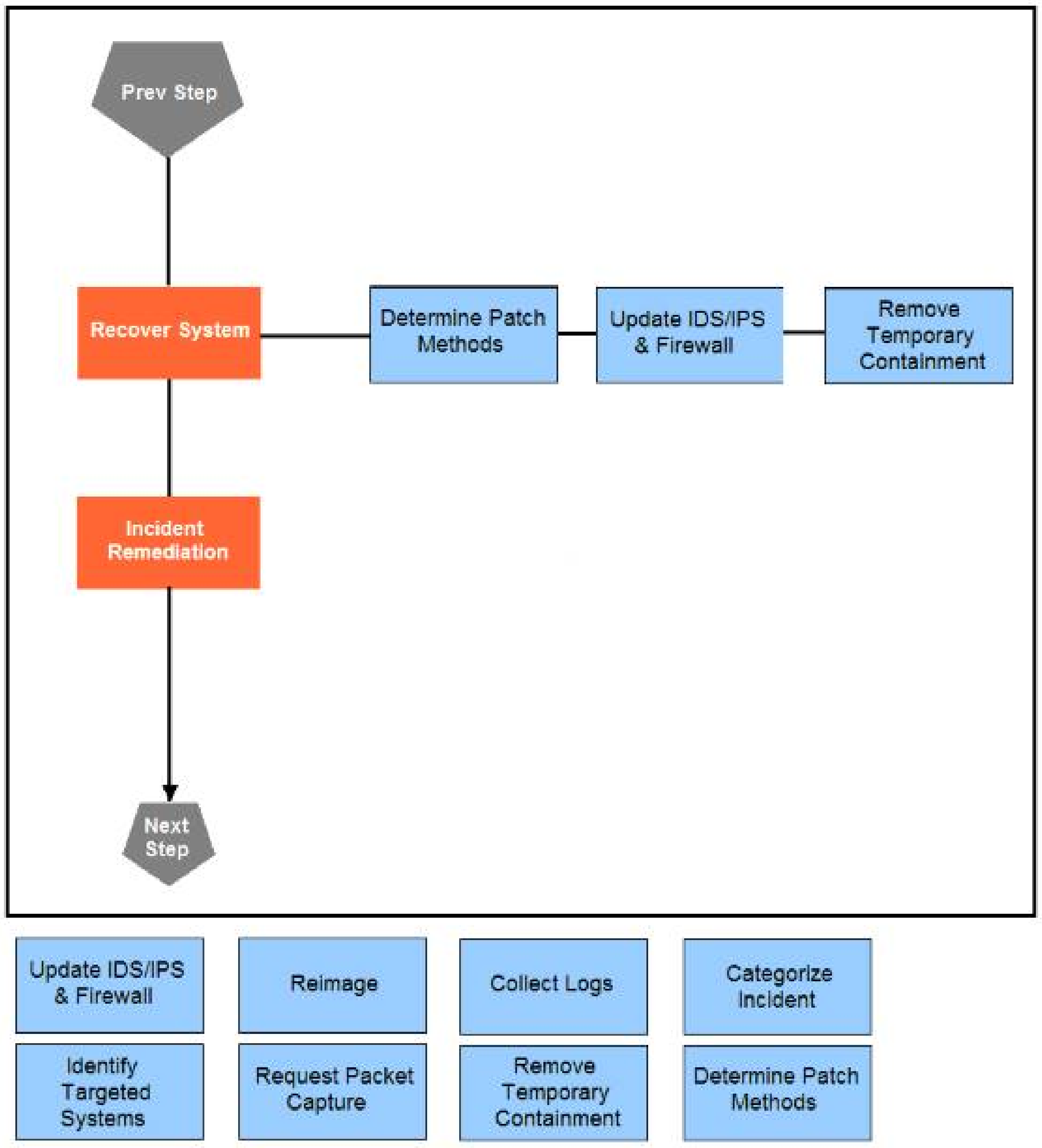
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 12
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

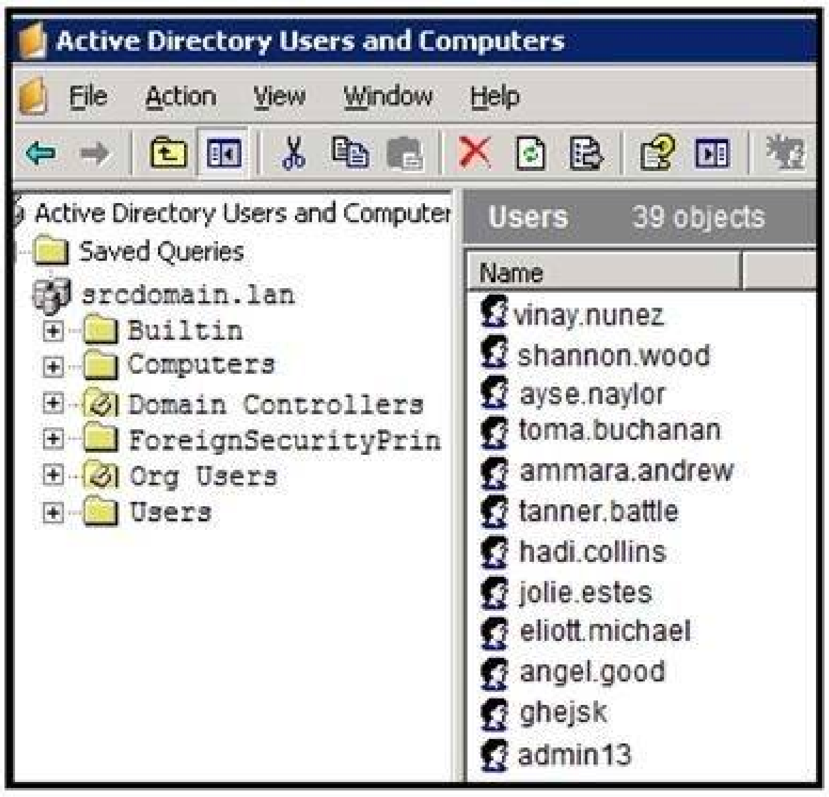
Answer: D

NEW QUESTION 16
What is a limitation of cyber security risk insurance?

A. It does not cover the costs to restore stolen identities as a result of a cyber attack
B. It does not cover the costs to hire forensics experts to analyze the cyber attack
C. It does not cover the costs of damage done by third parties as a result of a cyber attack
D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Answer: A

NEW QUESTION 17
Refer to the exhibit.



vinay.nunez
shannon.wood
ayse.naylor
toma.buchanan
ammara.andrew
tanner.battle
hadi.collins
jolie.estes
eliott.michael
angel.good
ghejsk
admin13

An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

A. compromised insider
B. compromised root access
C. compromised database tables
D. compromised network

Answer: D

NEW QUESTION 18
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 23
An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions
B. Unpack the file in a sandbox to see how it reacts
C. Research the malware online to see if there are noted findings
D. Disassemble the malware to understand how it was constructed

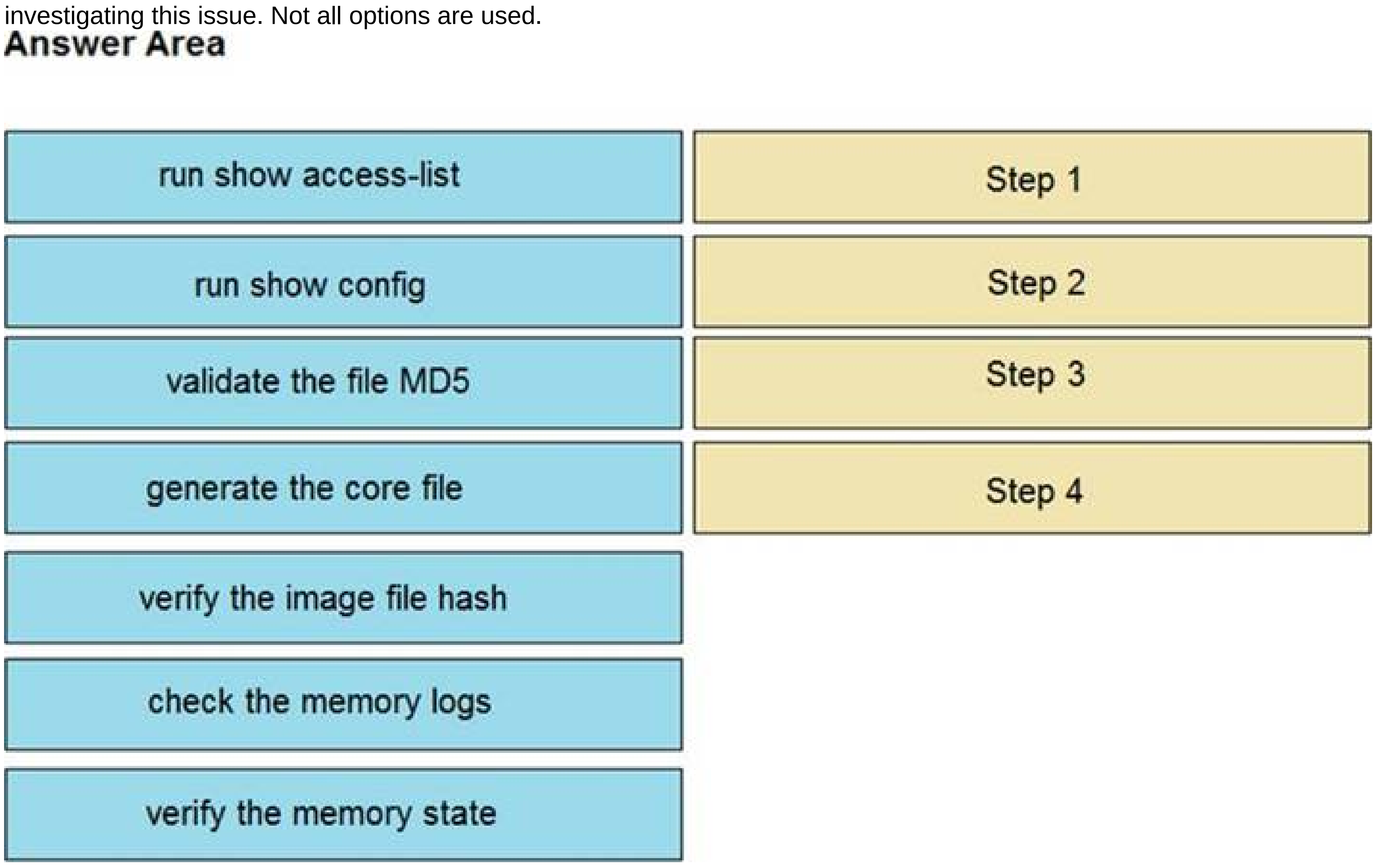
Answer: C

NEW QUESTION 26
A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

A. Classify the criticality of the information, research the attacker’s motives, and identify missing patches
B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

Answer: B

NEW QUESTION 28
An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.



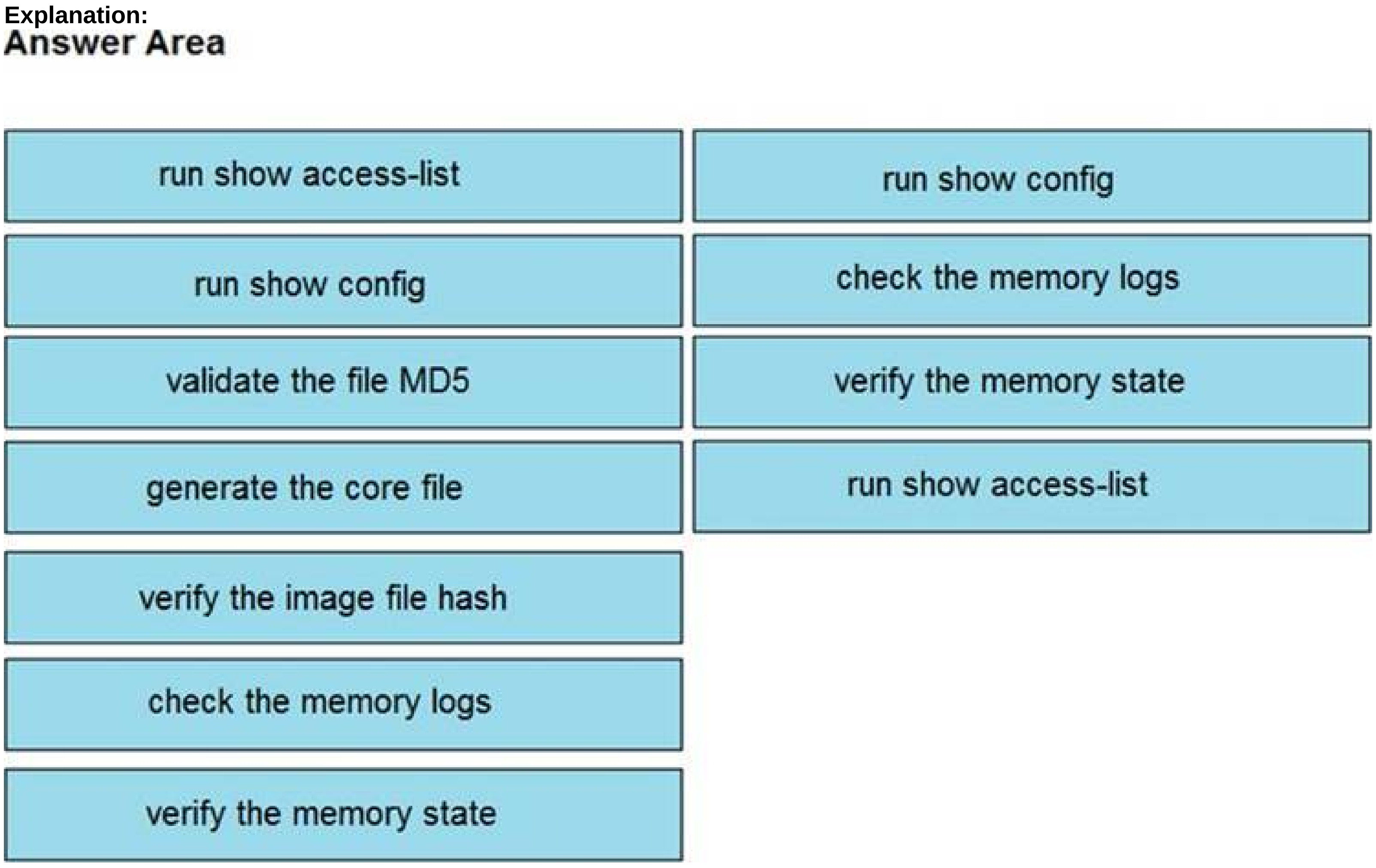
Answer Area

run show access-list	Step 1
run show config	Step 2
validate the file MD5	Step 3
generate the core file	Step 4
verify the image file hash	
check the memory logs	
verify the memory state	

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

run show access-list	run show config
run show config	check the memory logs
validate the file MD5	verify the memory state
generate the core file	run show access-list
verify the image file hash	
check the memory logs	
verify the memory state	

NEW QUESTION 33
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

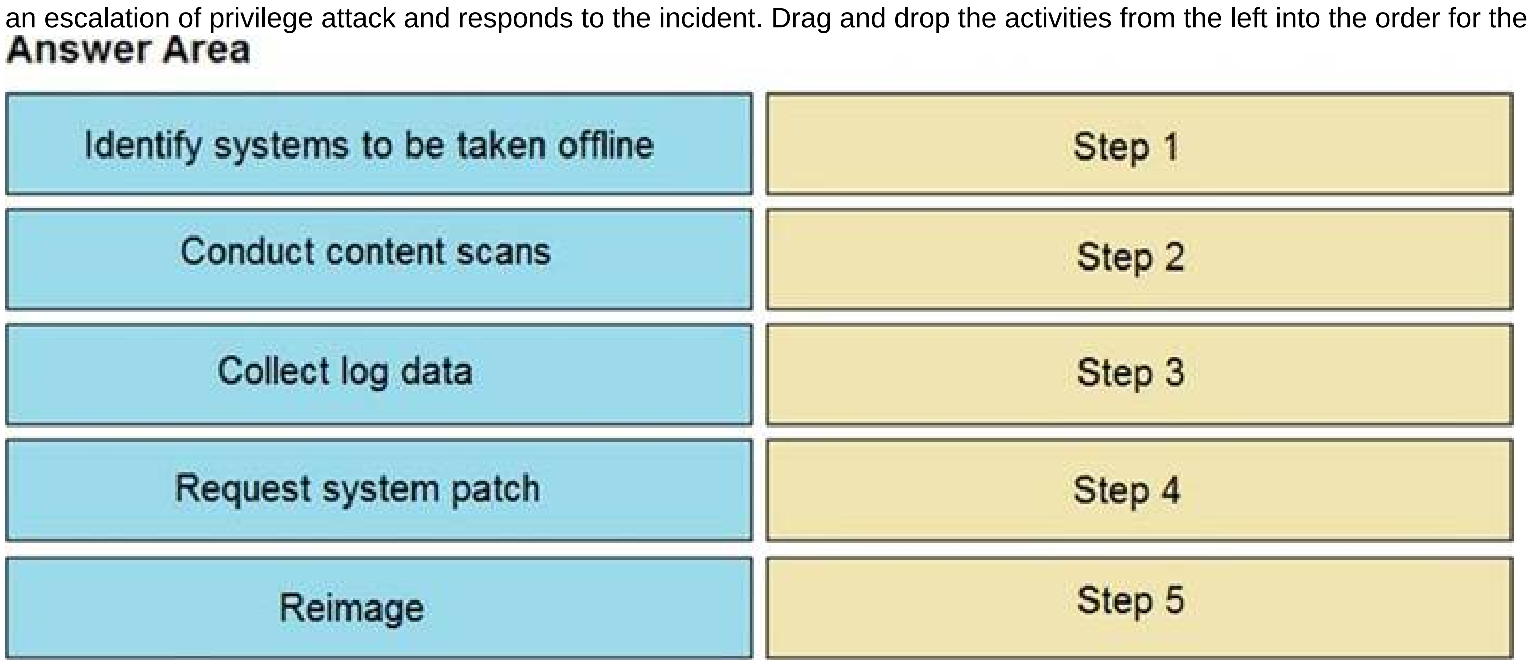
Answer: C

NEW QUESTION 35
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 39
An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response on the right.



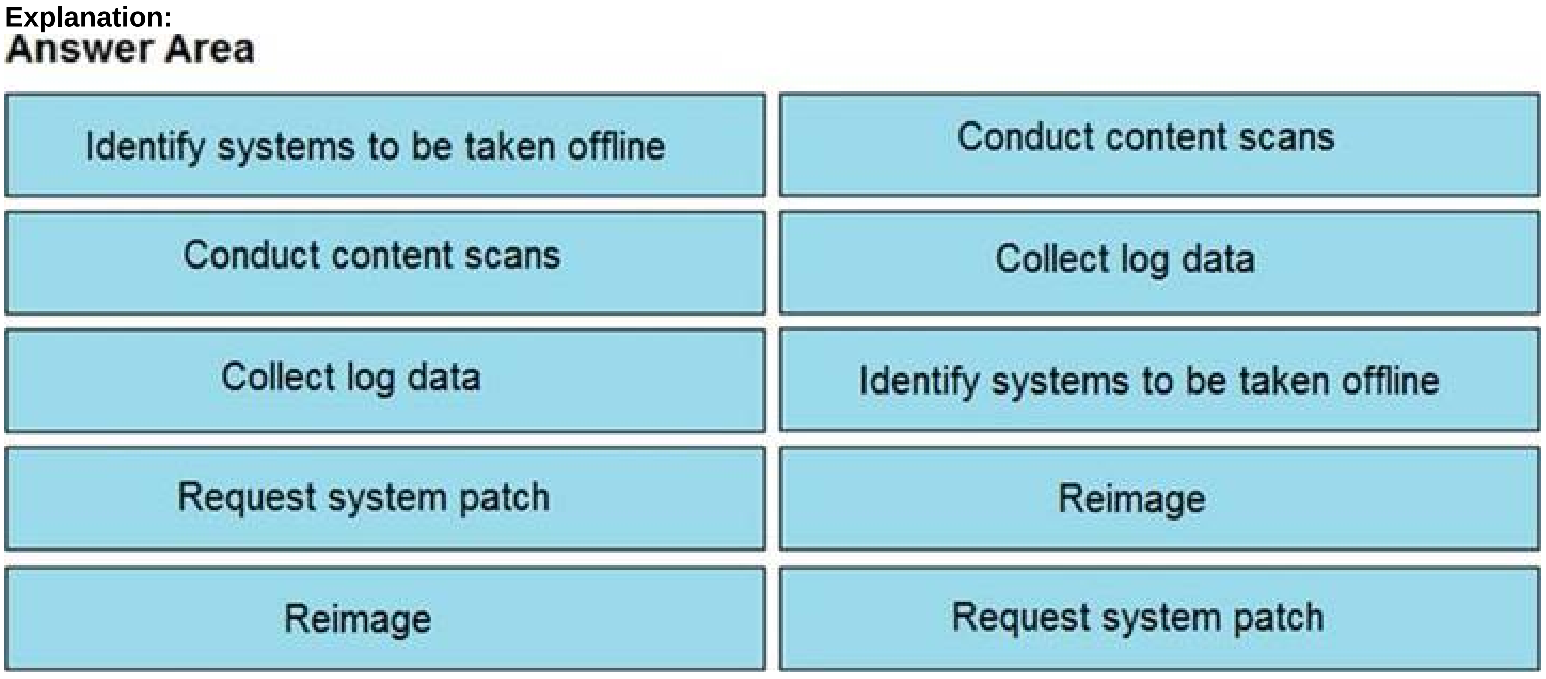
Answer Area

Identify systems to be taken offline	Step 1
Conduct content scans	Step 2
Collect log data	Step 3
Request system patch	Step 4
Reimage	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Identify systems to be taken offline	Conduct content scans
Conduct content scans	Collect log data
Collect log data	Identify systems to be taken offline
Request system patch	Reimage
Reimage	Request system patch

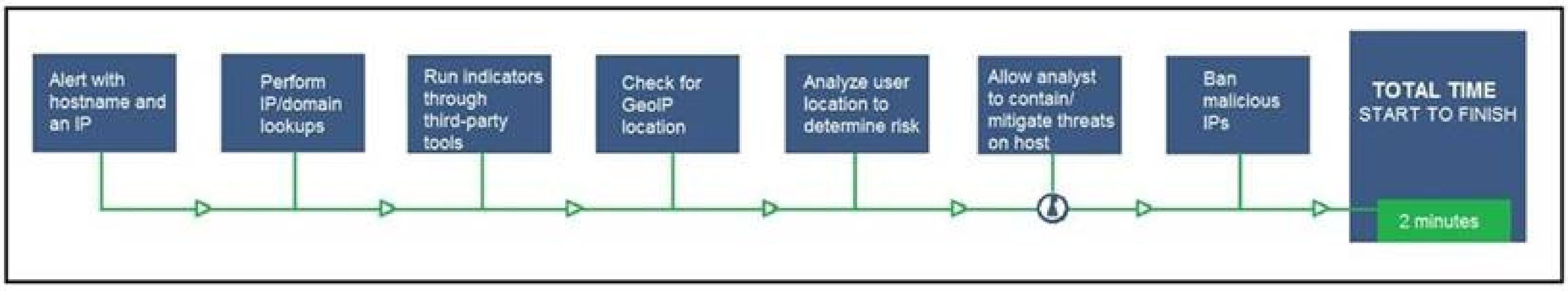
NEW QUESTION 40
An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

A. continuous delivery
B. continuous integration

C. continuous deployment
D. continuous monitoring

Answer: A

NEW QUESTION 44
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

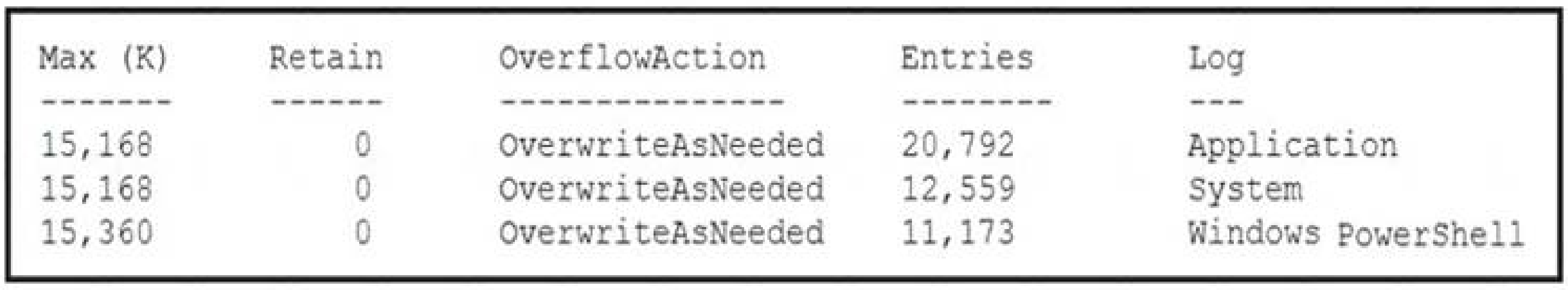
Answer: A

NEW QUESTION 46
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 50
Refer to the exhibit.



```
Max (K)   Retain   OverflowAction       Entries    Log
-------   ------   --------------       -------    ---
15,168         0   OverwriteAsNeeded    20,792     Application
15,168         0   OverwriteAsNeeded    12,559     System
15,360         0   OverwriteAsNeeded    11,173     Windows PowerShell
```

An employee is a victim of a social engineering phone call and installs remote access software to allow an
“MS Support” technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee’s laptop and the remote technician’s system?

A. No database files were disclosed
B. The database files were disclosed
C. The database files integrity was violated
D. The database files were intentionally corrupted, and encryption is possible

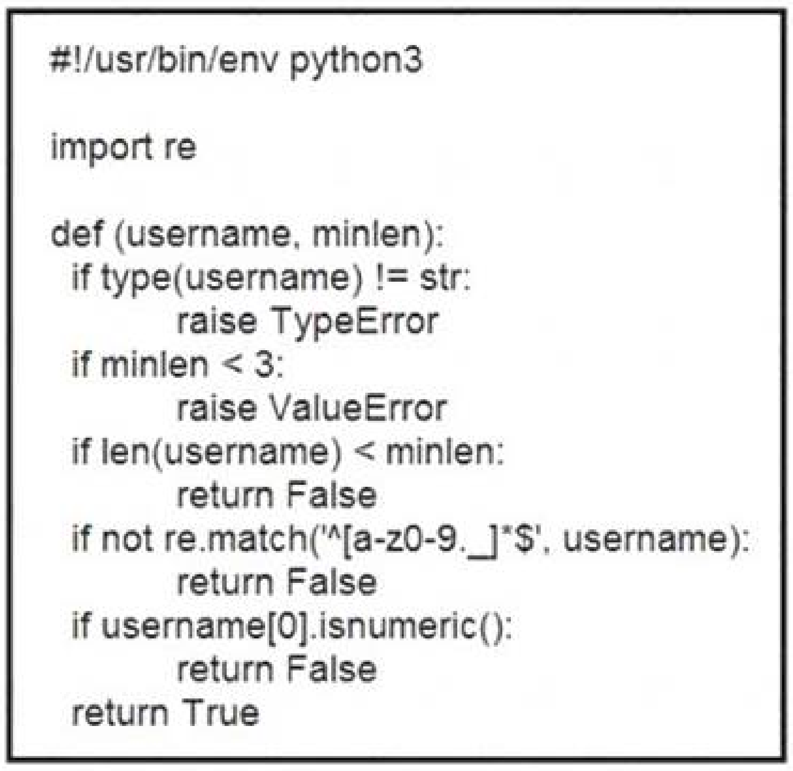
Answer: C

NEW QUESTION 53
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 58
Refer to the exhibit.



```
#!/usr/bin/env python3

import re

def (username, minlen):
  if type(username) != str:
         raise TypeError
  if minlen < 3:
         raise ValueError
  if len(username) < minlen:
         return False
  if not re.match('^[a-z0-9._]*$', username):
         return False
  if username[0].isnumeric():
         return False
  return True
```

An organization is using an internal application for printing documents that requires a separate registration on the website. The application allows format-free user creation, and users must match these required conditions to comply with the company's user creation policy:

- minimum length: 3
- usernames can only use letters, numbers, dots, and underscores
- usernames cannot begin with a number

The application administrator has to manually change and track these daily to ensure compliance. An engineer is tasked to implement a script to automate the process according to the company user creation policy. The engineer implemented this piece of code within the application, but users are still able to create format-free usernames. Which change is needed to apply the restrictions?

A. modify code to return error on restrictions def return false_user(username, minlen)
B. automate the restrictions def automate_user(username, minlen)
C. validate the restrictions, def validate_user(username, minlen)
D. modify code to force the restrictions, def force_user(username, minlen)

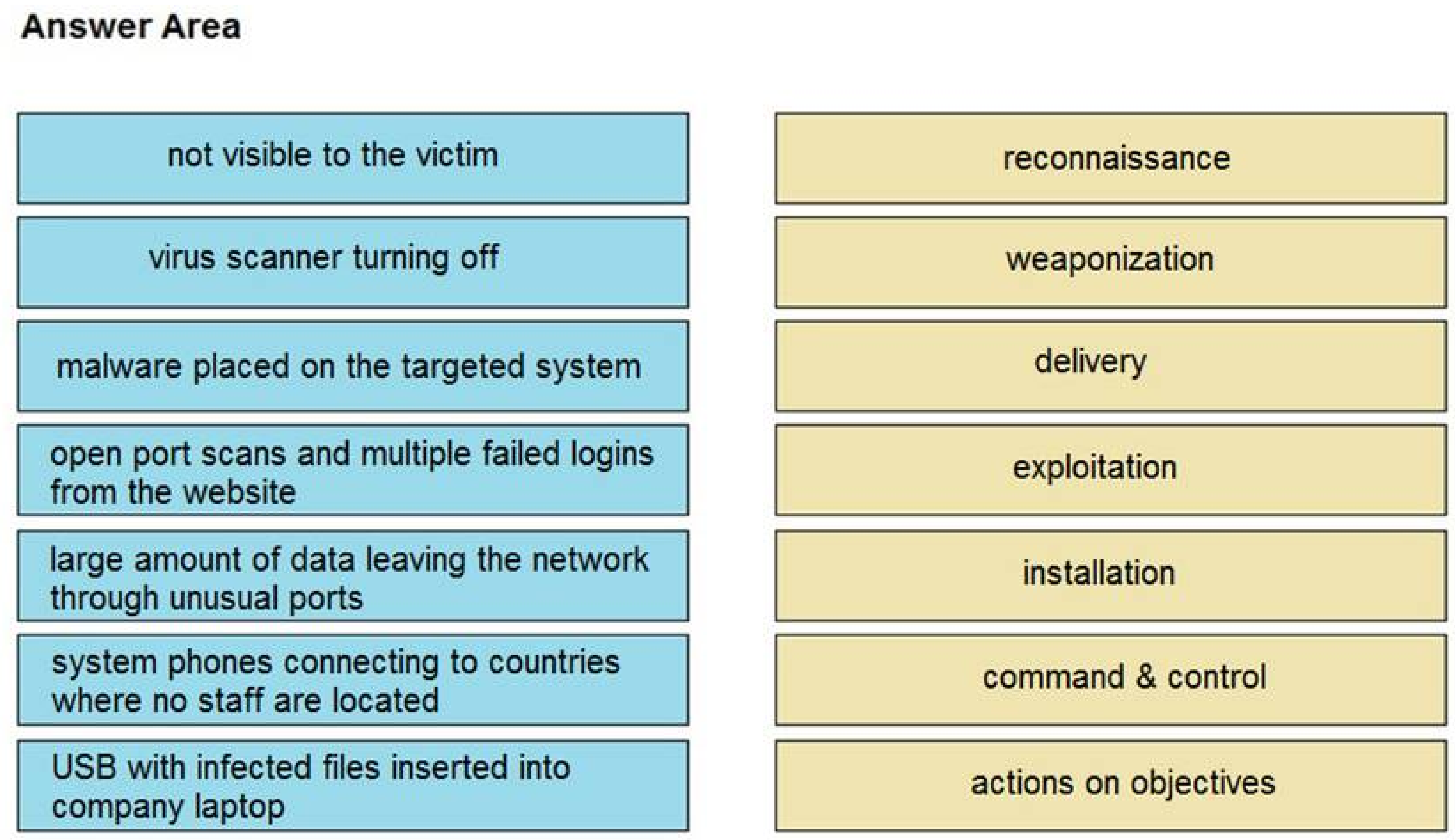
Answer: B

NEW QUESTION 62
A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

A. Mask PAN numbers
B. Encrypt personal data
C. Encrypt access
D. Mask sales details

Answer: B

NEW QUESTION 64
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.



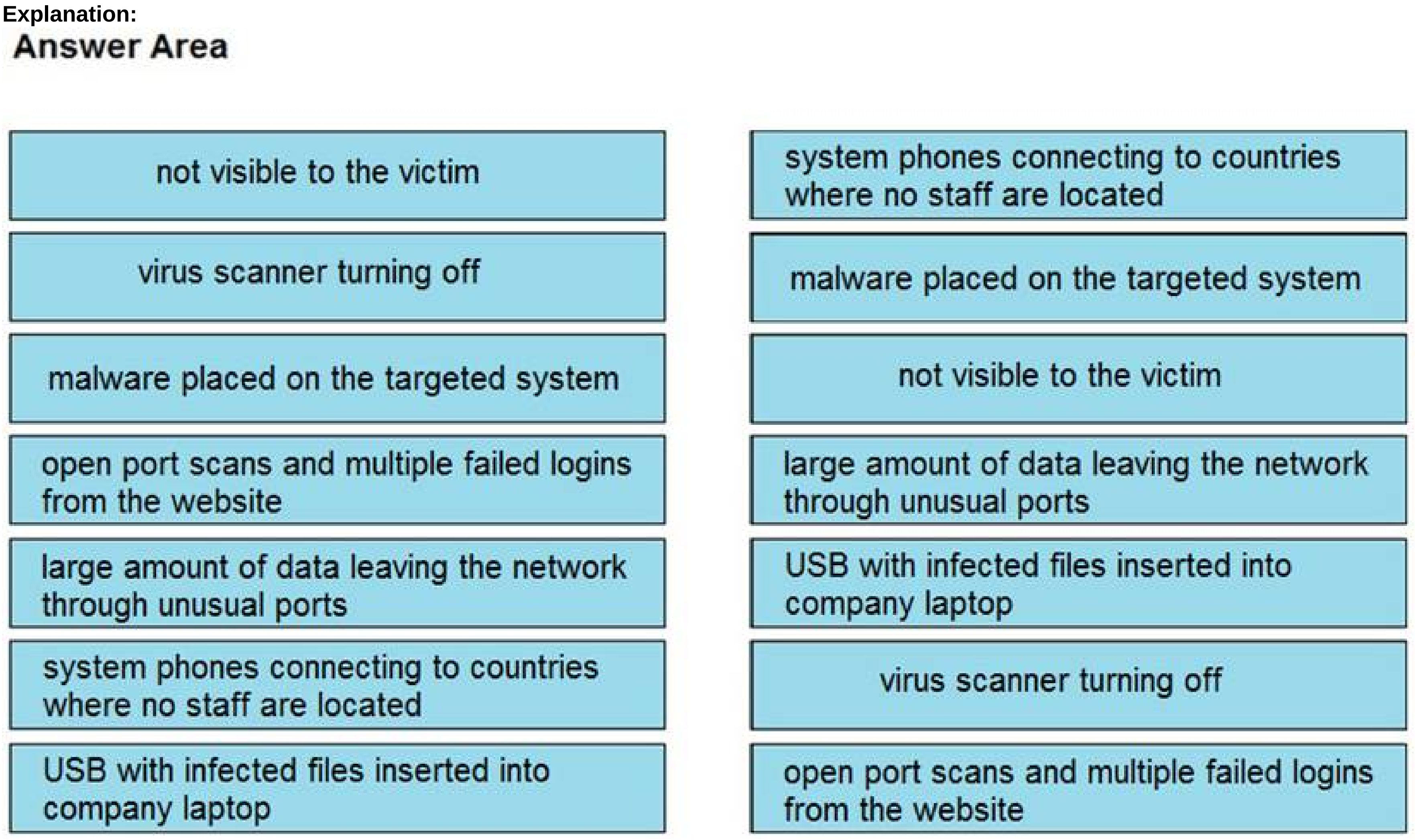
Answer Area

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

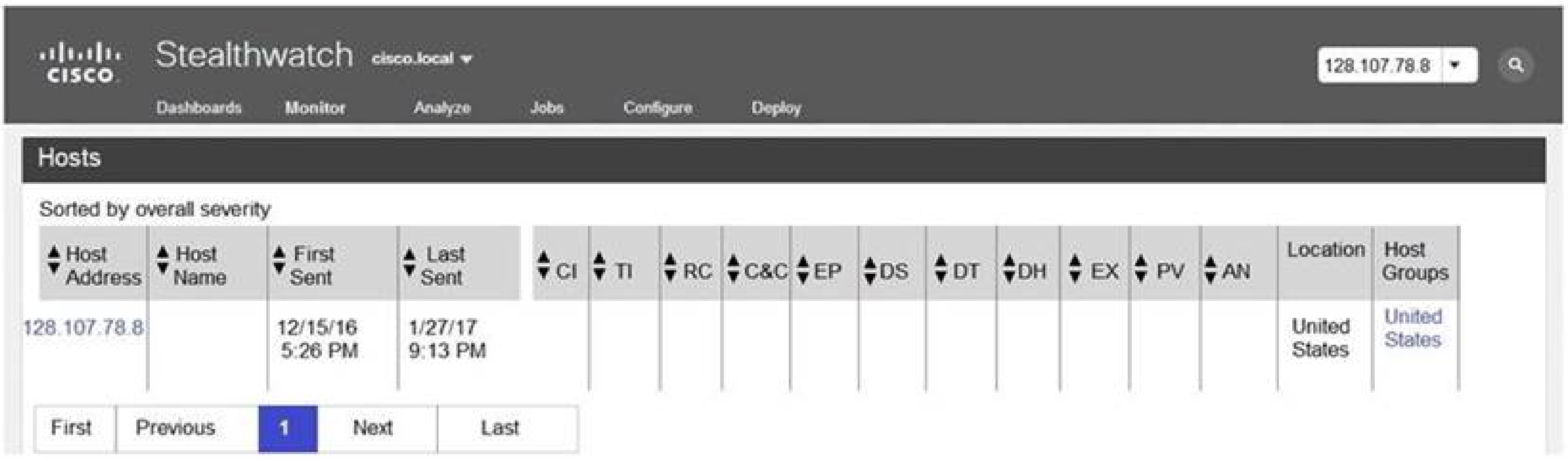
Explanation:



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 66
Refer to the exhibit.

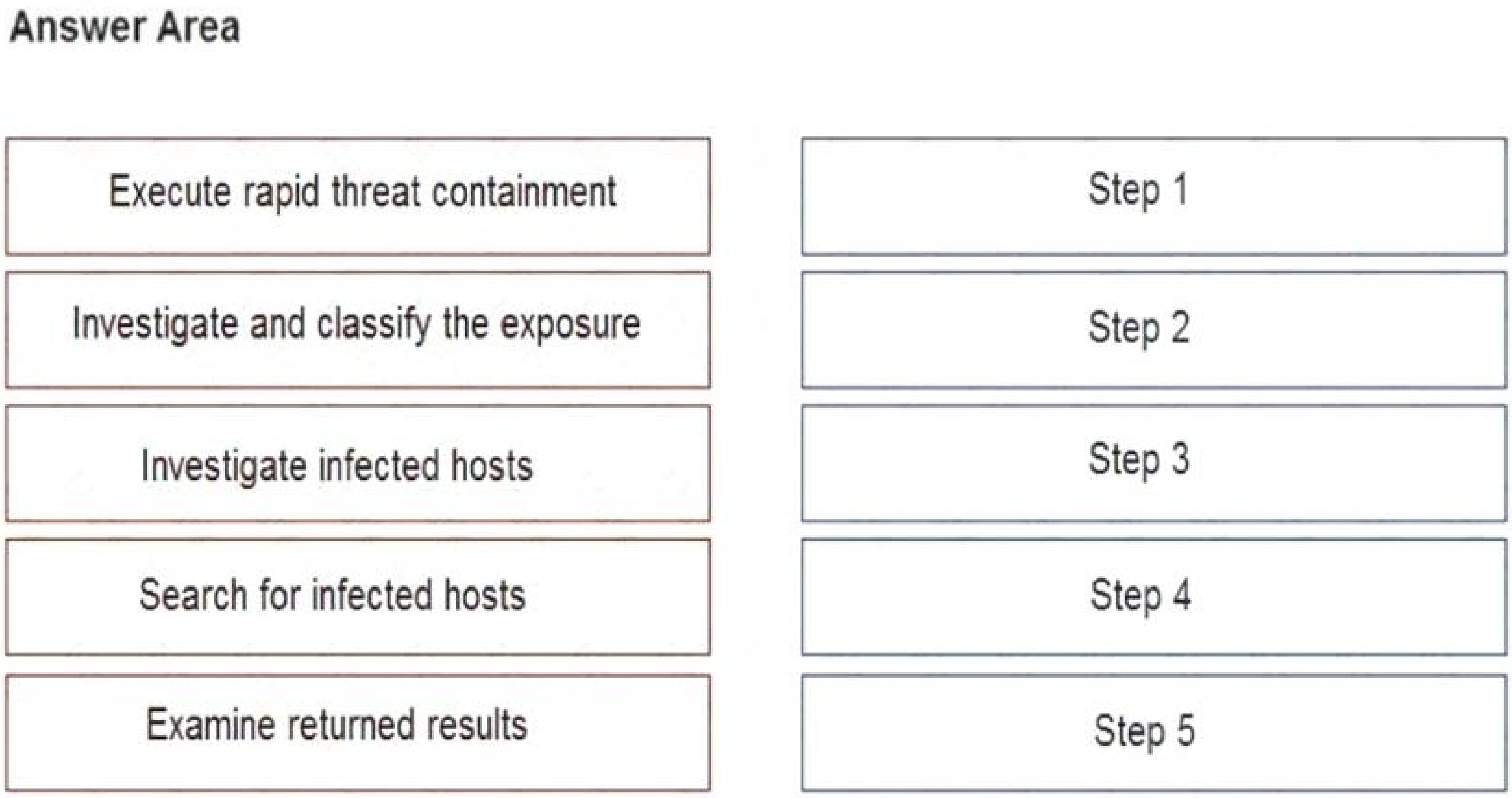


Hosts

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

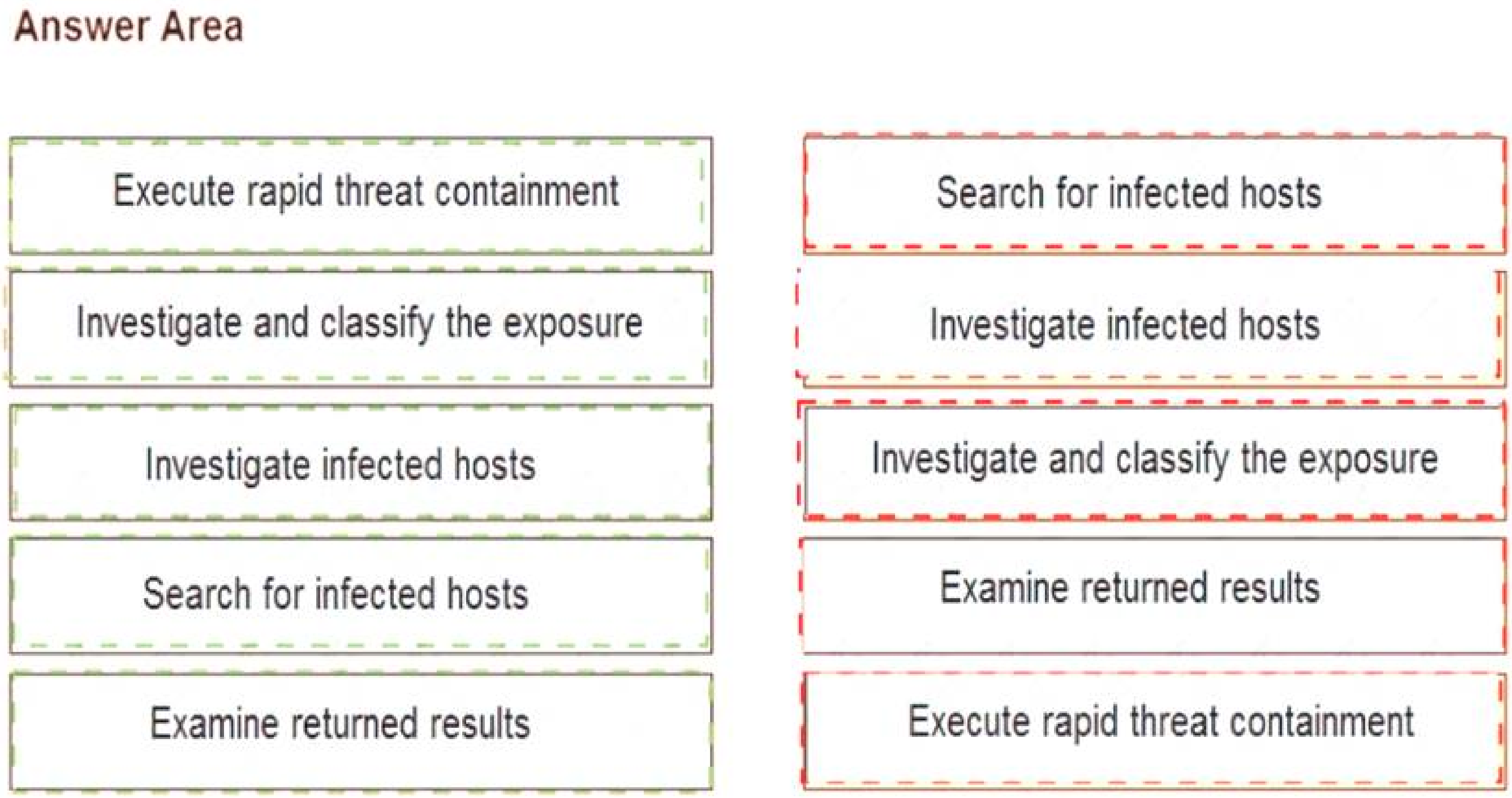
Step 4

Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Execute rapid threat containment

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Search for infected hosts

Investigate infected hosts

Investigate and classify the exposure

Examine returned results

Execute rapid threat containment

NEW QUESTION 70
Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

A. customer data
B. internal database
C. internal cloud
D. Internet

Answer: D

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

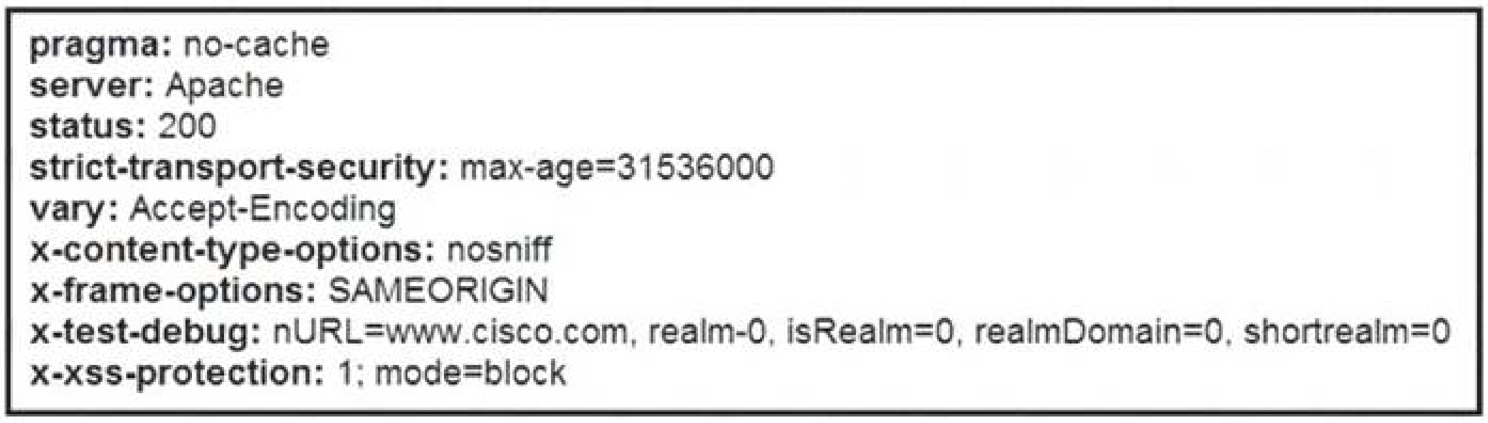
Answer: C

NEW QUESTION 74
A security expert is investigating a breach that resulted in a $32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack. Which step was missed that would have prevented this breach?

A. use of the Nmap tool to identify the vulnerability when the new code was deployed
B. implementation of a firewall and intrusion detection system
C. implementation of an endpoint protection system
D. use of SecDevOps to detect the vulnerability during development

Answer: D

NEW QUESTION 78
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 83
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 84
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 89

......

Relate Links

Contact us