CompTIA SY0-801 Dumps

Shared by Cruz on 26-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SIMULATION

Scenario: Threat intelligence analysis and compromised server remediation

You are a security operations analyst for a banking institution. Your main job function is to compare current, high-fidelity threat intelligence feeds to activity occurring on the bank's web server and customer relationship management (CRM) server.

The security operations center (SOC) has received multiple threat intelligence reports containing indicators of potentially malicious network activity.

You must review the available threat intelligence feeds, investigate the network connections and running processes on both servers, and remediate any confirmed compromise without interrupting legitimate banking services.

INSTRUCTIONS:

Click on each threat intelligence feed and console connection to:

* Review the appropriate threat intelligence feed.

* Determine if the servers are targeted.

* Remediate any compromise by stopping only the process connecting to bad hosts and removing the associated file.

Type help to view a list of available commands for each console.

If at any time you would like to return to the initial state of the simulation, click the Reset All button.

Exhibit 1 --- Original simulation interface

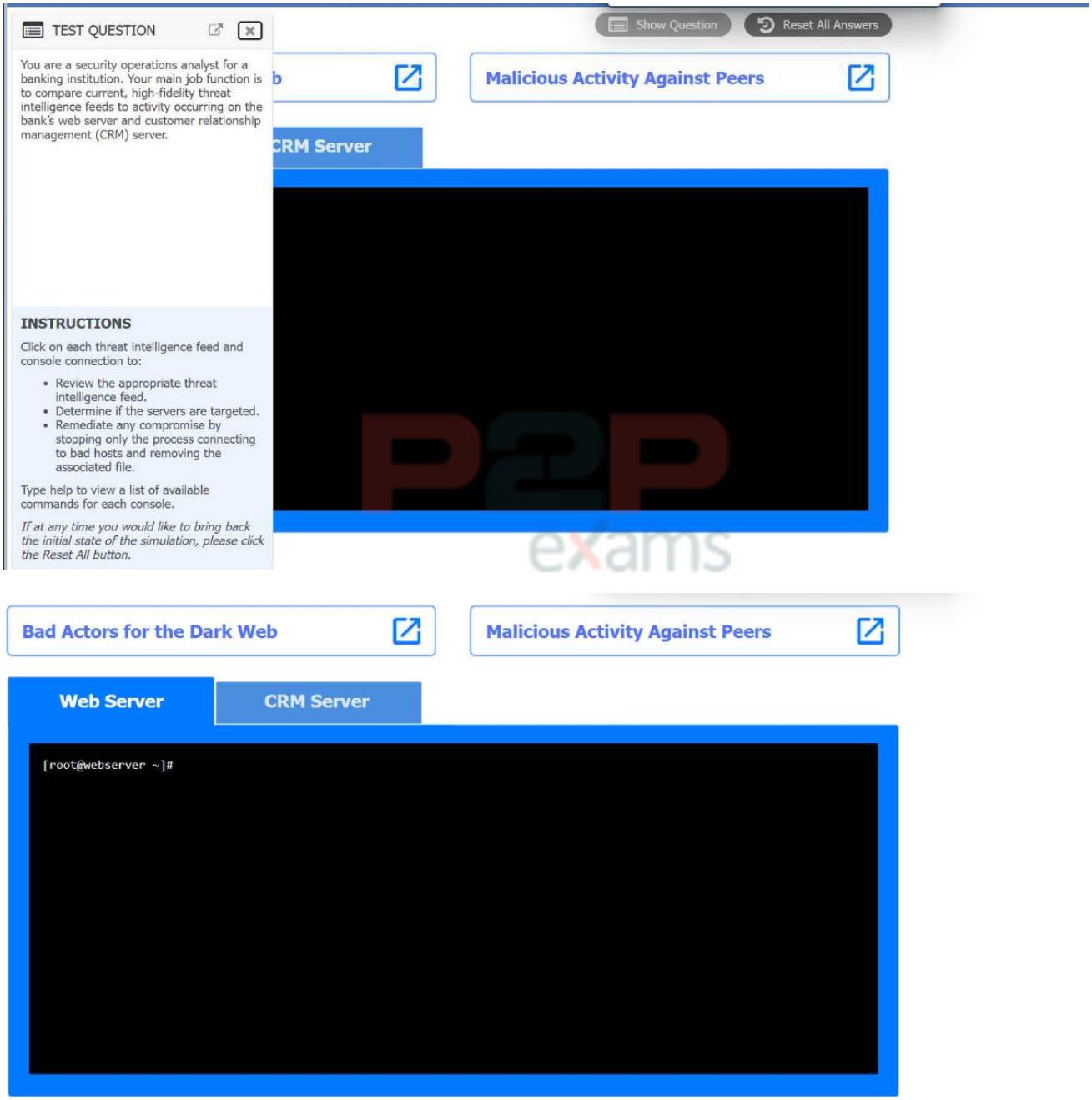
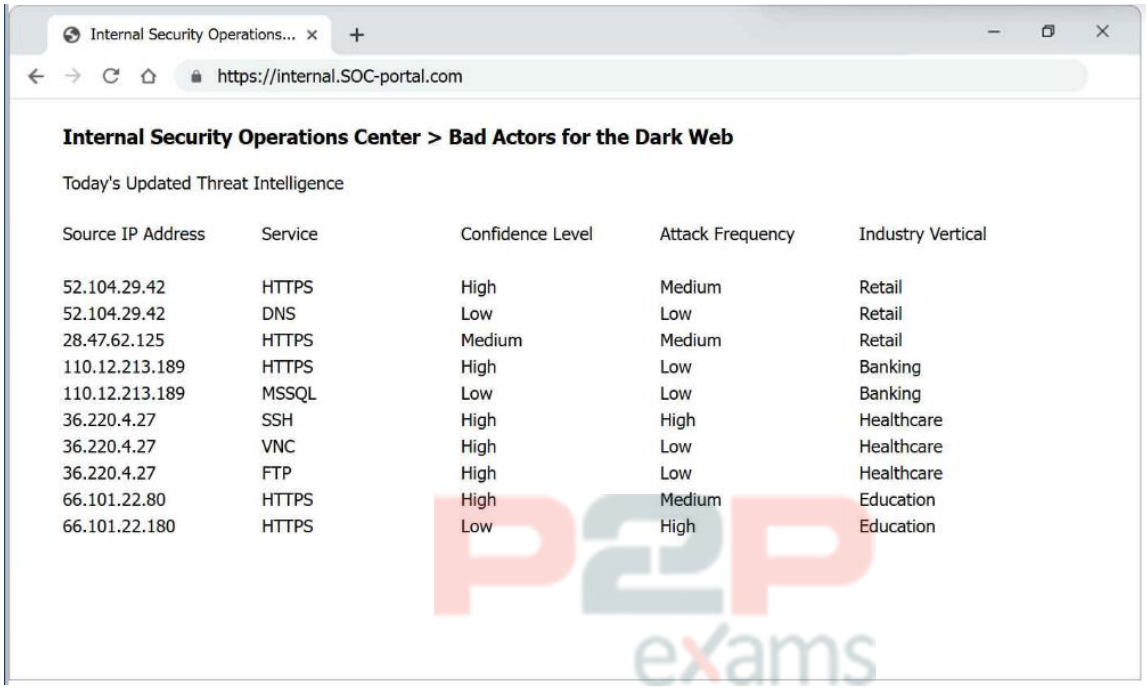


Exhibit 2 --- Bad Actors for the Dark Web

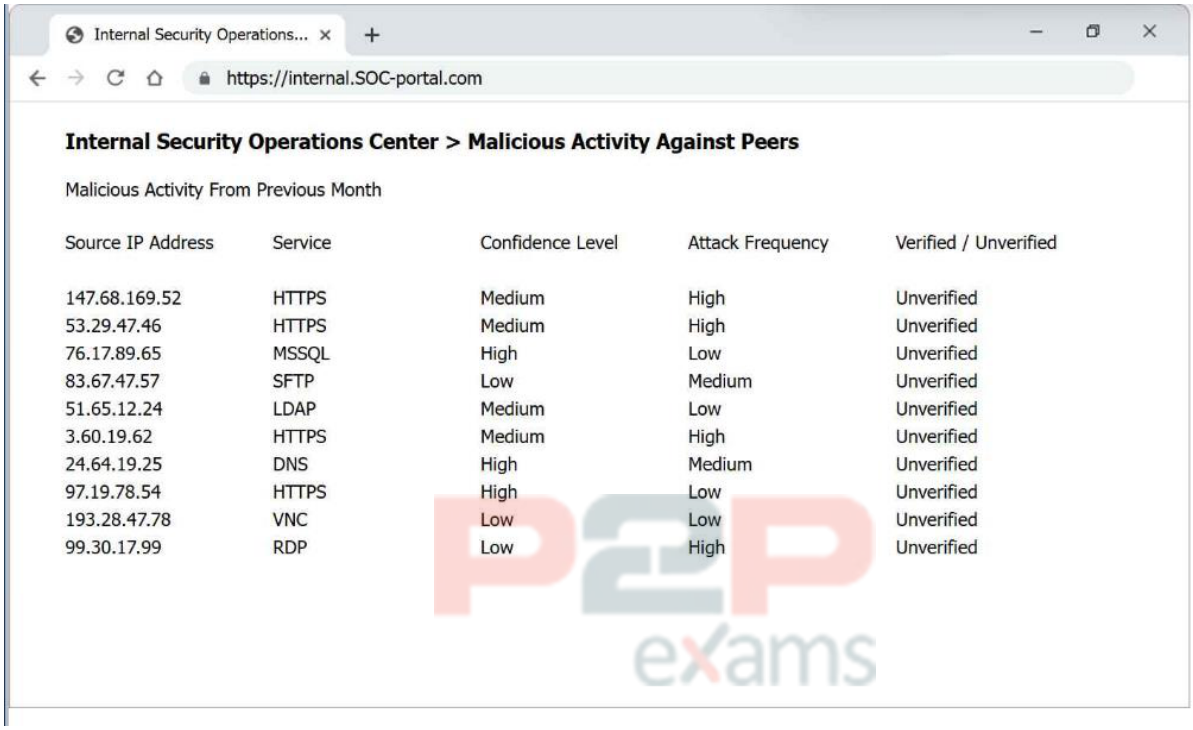
Internal Security Operations Center --- Today's Updated Threat Intelligence



Source IP address	Service	Confidence level	Attack frequency	Industry vertical
52.104.29.42	HTTPS	High	Medium	Retail
52.104.29.42	DNS	Low	Low	Retail
28.47.62.125	HTTPS	Medium	Medium	Retail
110.12.213.189	HTTPS	High	Low	Banking
110.12.213.189	MSSQL	Low	Low	Banking
36.220.4.27	SSH	High	High	Healthcare
36.220.4.27	VNC	High	Low	Healthcare
36.220.4.27	FTP	High	Low	Healthcare
66.101.22.80	HTTPS	High	Medium	Education
66.101.22.180	HTTPS	Low	High	Education

Exhibit 3 --- Malicious Activity Against Peers

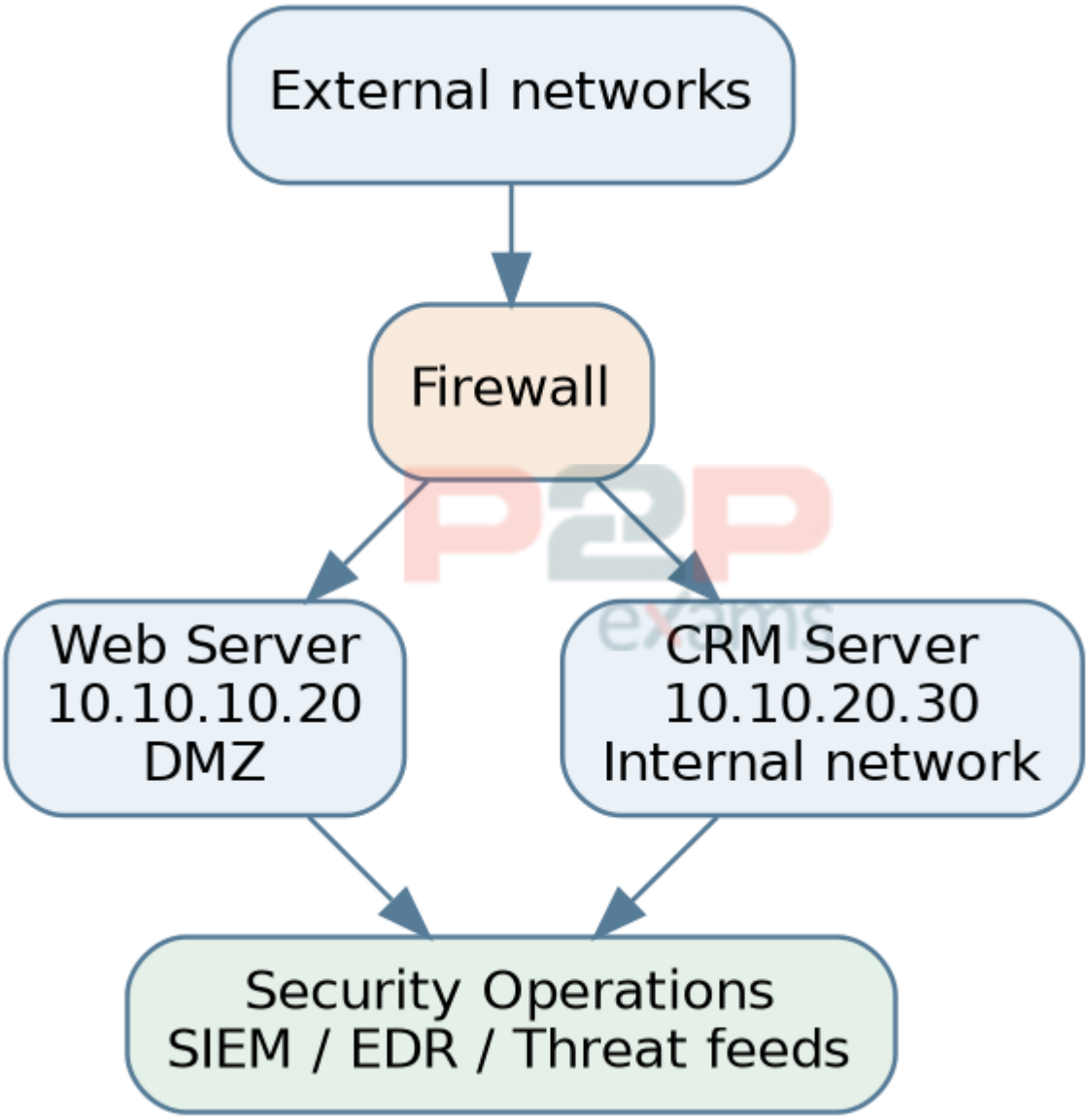
Internal Security Operations Center --- Malicious Activity from Previous Month



Source IP address	Service	Confidence level	Attack frequency	Verification
147.68.169.52	HTTPS	Medium	High	Unverified
53.29.47.46	HTTPS	Medium	High	Unverified
76.17.89.65	MSSQL	High	Low	Unverified
83.67.47.57	SFTP	Low	Medium	Unverified
51.65.12.24	LDAP	Medium	Low	Unverified
3.60.19.62	HTTPS	Medium	High	Unverified
24.64.19.25	DNS	High	Medium	Unverified
97.19.78.54	HTTPS	High	Low	Unverified
193.28.47.78	VNC	Low	Low	Unverified
99.30.17.99	RDP	Low	High	Unverified

Supplementary server evidence

Exhibit 4 --- Network infrastructure



Generated network topology for the reconstructed banking scenario.

Exhibit 5 --- Available console commands

Command	Purpose
help	Display available commands
ss -tunap	Display network connections and associated processes
ps -ef	Display running processes
ps -p PID -o pid,user,args	Inspect a specific process
readlink /proc/PID/exe	Identify the process executable
ls -l	Display file information
sha256sum	Calculate a file hash
kill PID	Request termination of a process
rm	Remove an identified file

These are illustrative Linux commands. The original simulator may implement a different subset of commands.

Exhibit 6 --- Web server active network connections

[root@webserver ~]# ss -tunap

State: ESTAB

Local: 10.10.10.20:443

Peer: 198.51.100.25:51022

Process: nginx, PID 812

State: ESTAB

Local: 10.10.10.20:51544

Peer: 110.12.213.189:443

Process: websync, PID 2458

State: ESTAB

Local: 10.10.10.20:49280

Peer: 10.10.30.10:443

Process: backup-agent, PID 1021

State: ESTAB

Local: 10.10.10.20:22

Peer: 10.10.40.15:56120

Process: sshd, PID 1190

[root@webserver ~]#

Exhibit 7 --- Web server running processes

Command executed: ps -ef

User	PID	Process or executable
root	812	/usr/sbin/nginx
backup	1021	/usr/local/bin/backup-agent
root	1190	/usr/sbin/sshd
www-data	2458	/tmp/.cache/websync
root	2490	/usr/sbin/rsyslogd

Exhibit 8 --- Web server endpoint security alert

Attribute	Recorded value
Hostname	webserver
Process	websync
PID	2458
Executable	/tmp/.cache/websync
Network destination	110.12.213.189
Destination port	TCP 443
Approved software inventory	No matching entry
File reputation	Confirmed malicious
Endpoint detection	Unauthorized command-and-control activity
Alert severity	Critical

The endpoint alert provides independent evidence that the suspicious network connection is associated with malicious activity.

Exhibit 9 --- CRM server active network connections

[root@crmserver ~]# ss -tunap

State: ESTAB

Local: 10.10.20.30:8443

Peer: 10.10.40.21:53120

Process: java, PID 1380

State: ESTAB

Local: 10.10.20.30:50211

Peer: 10.10.20.40:1433

Process: crm-service, PID 1450

State: ESTAB

Local: 10.10.20.30:51460

Peer: 110.12.213.189:1433

Process: crmupdate, PID 3176

State: ESTAB

Local: 10.10.20.30:22

Peer: 10.10.40.15:57011

Process: sshd, PID 1240

[root@crmserver ~]#

Exhibit 10 — CRM server running processes

Command executed: ps -ef

User	PID	Process or executable
root	1240	/usr/sbin/sshd
crm	1380	/usr/bin/java
crm	1450	/opt/crm/bin/crm-service
crm	3176	/var/tmp/.crm/crmupdate
root	3210	/usr/sbin/rsyslogd

Exhibit 11 — CRM server endpoint security alert

Attribute	Recorded value
Hostname	crmserver
Process	crmupdate
PID	3176
Executable	/var/tmp/.crm/crmupdate
Network destination	110.12.213.189
Destination port	TCP 1433
Approved software inventory	No matching entry
File reputation	Confirmed malicious
Endpoint detection	Unauthorized external database communication
Alert severity	Critical

Although the initial MSSQL threat intelligence record has low confidence, the endpoint security evidence confirms that the associated process is malicious in this reconstructed scenario.

Exhibit 12 --- Approved services and destinations

Server	Approved process	Approved service or destination
Web Server	nginx	Inbound HTTPS
Web Server	backup-agent	Internal backup server
Web Server	sshd	Authorized administration subnet
Web Server	rsyslogd	Centralized logging
CRM Server	java	Internal CRM application
CRM Server	crm-service	Internal database: 10.10.20.40:1433
CRM Server	sshd	Authorized administration subnet
CRM Server	rsyslogd	Centralized logging

Answer area --- Simulation console

Review the source threat intelligence and reconstructed console evidence. Select the malicious process and associated executable for each affected server.

Select the primary threat intelligence feed:

Bad Actors for the Dark Web --- Today's feed

Malicious Activity Against Peers --- Previous month

Web Server — process	Web Server — associated file
◻ 812 — nginx	◻ /usr/sbin/nginx
◻ 1021 — backup-agent	◻ /usr/local/bin/backup-agent
◻ 1190 — sshd	◻ /usr/sbin/sshd
◻ 2458 — websync	◻ /tmp/.cache/websync
◻ 2490 — rsyslogd	◻ /usr/sbin/rsyslogd

CRM Server — process	CRM Server — associated file
◻ 1240 — sshd	◻ /usr/sbin/sshd
◻ 1380 — java	◻ /usr/bin/java
◻ 1450 — crm-service	◻ /opt/crm/bin/crm-service
◻ 3176 — crmupdate	◻ /var/tmp/.crm/crmupdate
◻ 3210 — rsyslogd	◻ /usr/sbin/rsyslogd

Options:

A- See the Explanation for detailed Answer

Answer:

A

Explanation:

Step 1: Select the most relevant threat intelligence feed

Correct selection: Bad Actors for the Dark Web

The appropriate primary feed is today's updated threat intelligence because it provides current threat information and includes industry-specific classifications directly relevant to the banking organization.

Evaluation criterion	Dark Web feed	Peer activity feed
Freshness	Current	Previous month
Industry relevance	Banking-specific indicators available	Not specified
Confidence information	Available	Available
Explicitly marked unverified	Not specified	Yes
Investigation priority	Primary	Supplementary

The previous month's peer activity report remains useful for supplementary investigation, but it is less suitable as the primary source when investigating current threats.

Step 2: Identify indicators relevant to banking infrastructure

Filter the current threat intelligence feed for banking-related activity.

IP address	Service	Confidence	Priority
110.12.213.189	HTTPS	High	High
110.12.213.189	MSSQL	Low	Investigate

The HTTPS indicator warrants priority investigation because it combines current intelligence, high confidence, and banking industry relevance.

The MSSQL indicator requires additional corroboration before remediation because its confidence level is low.

Confidence and attack frequency are different attributes. Low attack frequency does not necessarily indicate a low-impact threat, while high attack frequency does not independently establish that an indicator is accurate.

Also, the original feed identifies source IP addresses, whereas the reconstructed console shows the same address as an outbound destination. That correlation warrants investigation but is not

independently sufficient to establish compromise.

Step 3: Investigate the web server

First, examine the network connections.

ss -tunap

Identify the following suspicious connection:

Attribute	Finding
Local host	10.10.10.20
Remote host	110.12.213.189
Destination port	443
Protocol	TCP
Connection state	ESTABLISHED
Process	websync
PID	2458

The remote IP address matches the high-confidence banking HTTPS threat intelligence record.

Inspect the associated process:

ps -p 2458 -o pid,user,args

Expected output:

PID USER COMMAND

2458 www-data /tmp/.cache/websync

Identify the executable:

readlink /proc/2458/exe

Expected output:

/tmp/.cache/websync

The executable is not part of the approved software inventory, and endpoint telemetry independently confirms malicious command-and-control activity.

Step 4: Remediate the web server

Preserve relevant endpoint alerts, connection records, executable hashes, and any evidence required by the organization's incident response policy before deleting the malicious file.

Calculate the file hash:

sha256sum /tmp/.cache/websync

After confirming the identity of the process, stop only the malicious process:

kill 2458

Verify that the process has terminated:

ps -p 2458

After evidence preservation and authorization, remove the malicious executable:

rm /tmp/.cache/websync

Verify that the suspicious network connection is no longer present:

ss -tunap

Web server remediation summary:

Action	Correct value
Targeted server	Web Server
Malicious IP	110.12.213.189
Malicious process	websync
Process ID	2458
Process action	Terminate
Malicious file	/tmp/.cache/websync
File action	Remove after evidence preservation

Do not terminate nginx, sshd, rsyslogd, or the approved backup agent.

Step 5: Investigate the CRM server

Examine the CRM server's current network connections.

ss -tunap

The following connection requires investigation:

Attribute	Finding
Local host	10.10.20.30
Remote host	110.12.213.189
Destination port	1433
Service	MSSQL
Connection state	ESTABLISHED
Process	crmupdate
PID	3176

Port TCP 1433 is commonly associated with Microsoft SQL Server.

The CRM server's legitimate database is located at the internal address 10.10.20.40. The unauthorized external MSSQL communication is inconsistent with the approved connectivity policy.

Inspect the associated process:

ps -p 3176 -o pid,user,args

Expected output:

PID USER COMMAND

3176 crm /var/tmp/.crm/crmupdate

Identify the executable:

readlink /proc/3176/exe

Expected output:

/var/tmp/.crm/crmupdate

Although the threat feed assigns low confidence to the MSSQL indicator, the unauthorized executable, unexpected external connection, and corroborating endpoint alert collectively establish a confirmed compromise within the reconstructed scenario.

Step 6: Remediate the CRM server

Preserve the required forensic evidence before removing the file.

Calculate the malicious executable's hash:

sha256sum /var/tmp/.crm/crmupdate

Terminate only the confirmed malicious process:

kill 3176

Verify that the process has terminated:

ps -p 3176

Remove the malicious file after evidence preservation:

rm /var/tmp/.crm/crmupdate

Verify the network connection has been eliminated:

ss -tunap

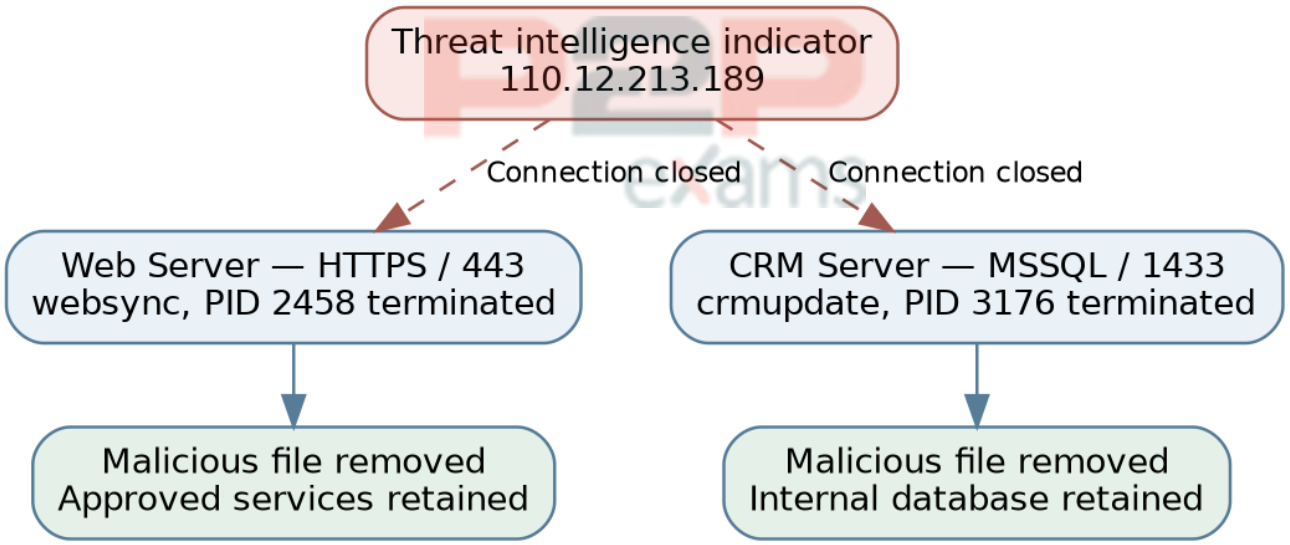
Confirm that the legitimate internal database connection remains available.

CRM server remediation summary:

Action	Correct value
Targeted server	CRM Server
Malicious IP	110.12.213.189
Malicious process	crmupdate
Process ID	3176
Process action	Terminate
Malicious file	/var/tmp/.crm/crmupdate
File action	Remove after evidence preservation

Do not terminate the legitimate crm-service process using PID 1450. Doing so could interrupt access to the organization's approved database.

Step 7: Verify the completed remediation



Completed answer exhibit

Configuration	Web Server	CRM Server
Compromised	Yes	Yes
Threat intelligence feed	Today's Dark Web feed	Today's Dark Web feed
Suspicious remote IP	110.12.213.189	110.12.213.189
Service	HTTPS	MSSQL
Destination port	443	1433
Malicious process	websync	crmupdate
PID	2458	3176
Termination command	kill 2458	kill 3176
Associated file	/tmp/.cache/websync	/var/tmp/.crm/crmupdate
Required action	Stop process and remove file	Stop process and remove file

Web Server --- illustrative expected console results

[root@webserver ~]# kill 2458

[root@webserver ~]# rm /tmp/.cache/websync

[root@webserver ~]# ps -p 2458

PID TTY TIME CMD

Verification: process absent

Malicious connection: closed

Approved services: operational

CRM Server --- illustrative expected console results

[root@crmserver ~]# kill 3176

[root@crmserver ~]# rm /var/tmp/.crm/crmupdate

[root@crmserver ~]# ps -p 3176

PID TTY TIME CMD

Verification: process absent

Malicious connection: closed

Internal database: operational

Step 8: Perform post-remediation security checks

Terminating malicious processes and removing executable files satisfies the immediate

simulation requirements. However, these actions alone do not establish that a compromised server has been fully restored to a trustworthy state.

The SOC should investigate persistence mechanisms, review privileged account activity, search for additional indicators of compromise, assess potential data exfiltration, validate system integrity, and determine whether recovery from a trusted system image is necessary.

Any containment decisions should minimize business disruption while preventing further unauthorized communications.

Question 2

Question Type: MultipleChoice

SIMULATION

Scenario: Compromised employee accounts, password security, and access management

An organization has learned that its data is being exchanged on the dark web. The CIO has requested that you investigate and implement the most secure solution to protect employee accounts.

As part of the investigation, you must examine the organizational directory, compensation report, and user account information to identify inappropriate access permissions and weak password practices.

The organization requires a role-based access control solution and a secure authentication mechanism to protect sensitive information and prevent further account compromise.

INSTRUCTIONS:

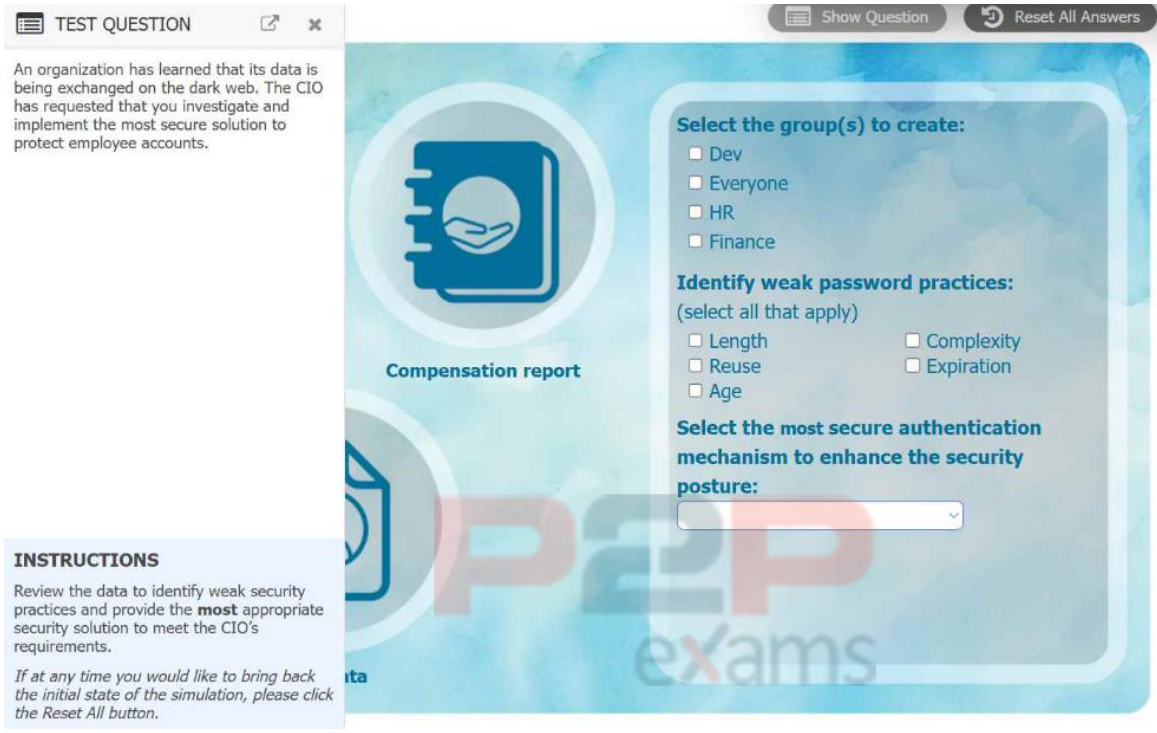
Review the data to identify weak security practices and provide the most appropriate security solution to meet the CIO's requirements.

* Examine the directory contents, compensation report, and user data.

* Select the appropriate groups to create.

* Identify all applicable weak password practices.

* Select the most secure authentication mechanism.





Supplementary scenario evidence: The PDF displays the three evidence icons but does not show the contents of the windows they open. The following exhibits have been generated specifically to complete the original simulation and provide a defensible answer configuration.

Exhibit 2 --- Directory contents

The security administrator discovers the following directory structure and existing permissions.

Directory	Existing access group	Current permission	Classification
/Company/Public	Everyone	Read	Public
/Company/Development	Everyone	Read/Write	Confidential
/Company/HR	Everyone	Read/Write	Restricted
/Company/Finance	Everyone	Read/Write	Restricted
/Company/HR/Compensation	Everyone	Read/Write	Restricted
/Company/Finance/Payroll	Everyone	Read/Write	Restricted

The Everyone group is already present. Sensitive directories currently inherit excessive permissions from this group.

Exhibit 3 --- Compensation report

Classification: Restricted

Employee ID	Employee	Department	Annual salary
EMP001	James Wilson	Dev	$92,000
EMP002	Rebecca Smith	HR	$76,000
EMP003	Daniel Brown	Finance	$84,000
EMP004	Sarah Johnson	Dev	$88,000
EMP005	David Miller	Finance	$81,000
EMP006	Emily Davis	HR	$72,000

Current access permission: Everyone --- Read/Write.

Authorized personnel: HR compensation administrators and designated payroll staff only.

The compensation report contains sensitive employee financial information that should not be accessible to the general workforce.

Exhibit 4 --- User data and password audit

The administrator reviews the following password audit results. Password metadata and reuse indicators are provided instead of exposing plaintext passwords.

Username	Department	Password length	Password reused	Compromised password detected	Password age
jwilson	Dev	6	Yes	Yes	180 days
rsmith	HR	7	Yes	Yes	90 days
dbrown	Finance	8	No	Yes	365 days
sjohnson	Dev	6	Yes	Yes	120 days
dmiller	Finance	16	Yes	Yes	60 days
edavis	HR	20	No	No	45 days

Exhibit 5 --- Current authentication policy

Policy setting	Current configuration
Authentication method	Password only
Minimum password length	6 characters
Maximum supported length	64 characters
Compromised password screening	Disabled
Password reuse restrictions	Disabled
Scheduled password expiration	Not enforced
Multifactor authentication	Disabled
Account lockout	Enabled
Password change after compromise	Required by incident response policy
Failed authentication monitoring	Enabled

Answer area

Select the group(s) to create:

Dev Everyone HR Finance

Identify weak password practices (select all that apply):

Length Complexity Reuse Expiration Age

Select the most secure authentication mechanism:

PIN Credential manager Passkey SMS code

Options:

A- See the Explanation for detailed Answer

Answer:

A

Explanation:

Step 1: Create the appropriate security groups

The organization should create the following department-specific security groups.

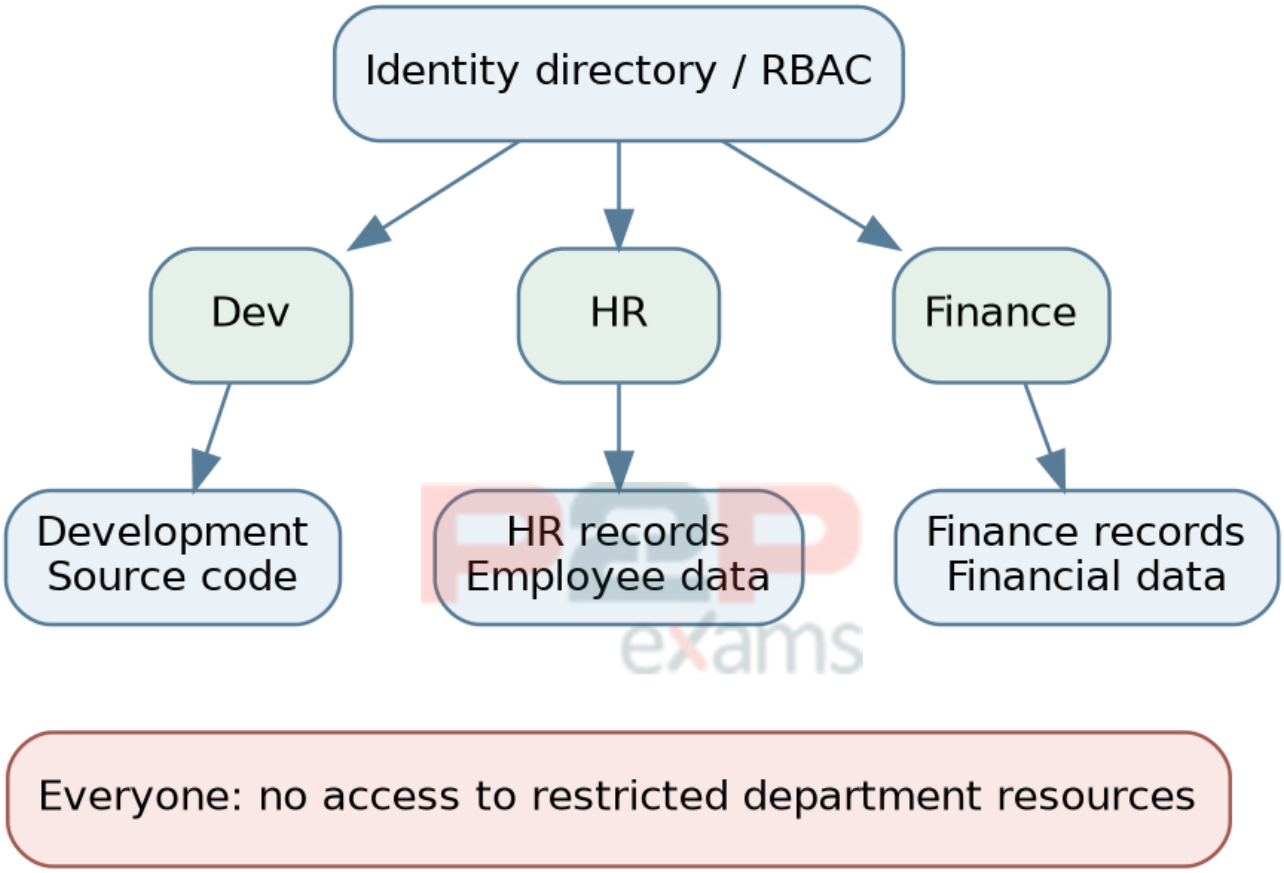
Group	Selection
Dev	Selected
Everyone	Not selected
HR	Selected
Finance	Selected

The existing Everyone group provides excessively broad permissions to confidential and restricted information.

Implementing role-based access control (RBAC) enables permissions to be assigned according to departmental responsibilities rather than individual exceptions or unrestricted organizational membership.

Step 2: Implement least-privilege access permissions

The following access model should be established.



Recommended permissions matrix:

Resource	Dev	HR	Finance	Everyone
Public	Read	Read	Read	Read
Development	Read/Write	Denied	Denied	Denied
HR	Denied	Read/Write	Denied	Denied
Finance	Denied	Denied	Read/Write	Denied
Compensation	Denied	Authorized subset	Denied	Denied
Payroll	Denied	Authorized subset	Authorized subset	Denied

Access to payroll and compensation information should be restricted further through dedicated permissions for authorized individuals. Membership in the finance or HR department alone does not necessarily justify access to every sensitive employee record.

This approach implements least privilege, need-to-know authorization, and segregation of duties.

Step 3: Identify weak password practices

Password practice	Selection	Explanation
Length	Selected	The six-character minimum is insufficient.
Complexity	Not selected	The evidence does not establish a separate complexity deficiency.
Reuse	Selected	Multiple compromised passwords are reused.
Expiration	Not selected	Routine password expiration is not inherently required.
Age	Not selected	Password age alone does not establish insecurity.

The password audit clearly identifies two deficiencies: insufficient password length and credential reuse.

The organization must enforce longer passwords, screen proposed passwords against known compromised values, and reset credentials confirmed to have been exposed.

Important technical distinction: Current NIST SP 800-63B-4 guidance requires a minimum of 15 characters for passwords used as a single authentication factor. It does not require arbitrary character-composition rules or routine password changes without evidence of compromise. Consequently, selecting every password characteristic as a weakness would not be defensible based on the reconstructed evidence.

Step 4: Select the most secure authentication mechanism

Correct selection: Passkey

Available mechanism	Security assessment
PIN	May be useful for locally unlocking an authenticator, but insufficient as a standalone remote authentication mechanism.
Credential manager	Improves password storage and generation but does not independently eliminate password phishing.
Passkey	Phishing-resistant public-key authentication using FIDO2/WebAuthn.
SMS code	Vulnerable to phishing, interception, and SIM-swapping attacks.

Exhibit 6 --- Passkey authentication workflow



Passkeys use public-key cryptography. The authentication service registers a public key, while the corresponding private key remains under the control of the authenticator or its approved synchronization mechanism.

Authentication requires cryptographic proof associated with the legitimate relying party, substantially reducing the risk of credential phishing. User verification may also require a local biometric or device PIN.

Passkeys are the strongest available authentication option in this simulation.

Step 5: Complete the simulation

Answer area	Completed selection
Groups to create	Dev, HR, Finance
Weak password practices	Length, Reuse
Authentication mechanism	Passkey

Step 6: Remediate compromised accounts

The organization should follow a controlled incident response process:

1. Identify accounts associated with exposed credentials.

2. Revoke suspicious sessions and authentication tokens.

3. Reset compromised passwords using trusted account recovery procedures.

4. Investigate unauthorized access to compensation and payroll information.

5. Remove excessive Everyone group access from restricted resources.

6. Assign users to appropriate role-based security groups.

7. Enroll employees in phishing-resistant passkey authentication.

8. Enable compromised credential screening and continuous authentication monitoring.

9. Verify group memberships, effective permissions, and access restrictions.

10. Document the incident and assess applicable data breach notification obligations.

Question 3

Question Type: MultipleChoice

SIMULATION

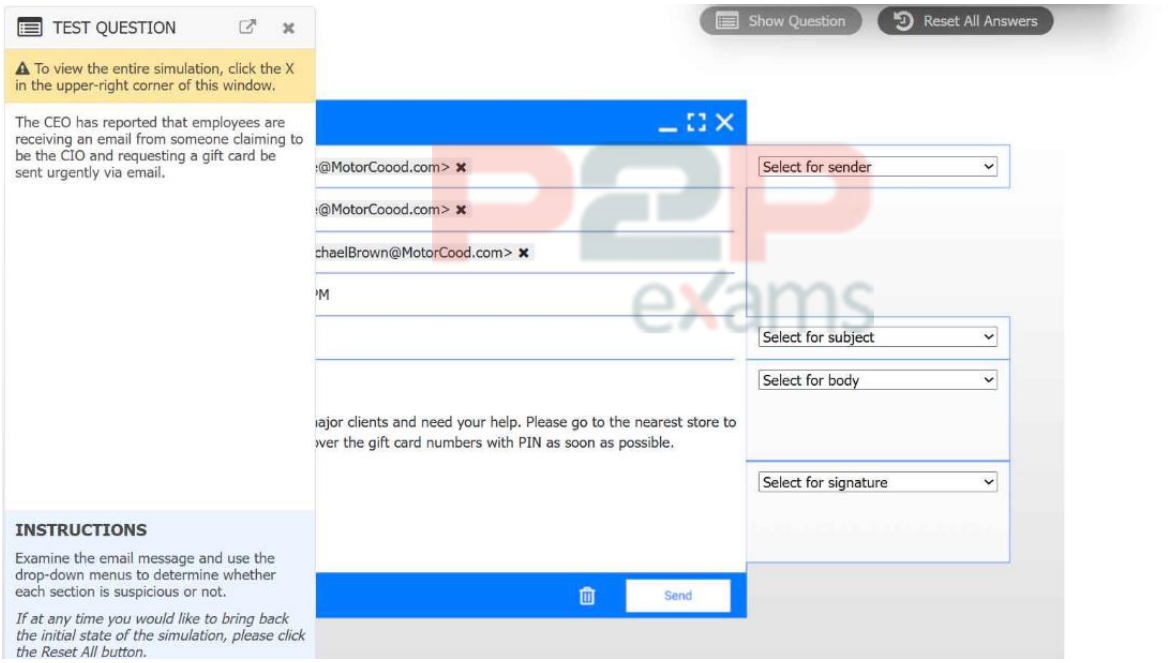
Scenario: Executive impersonation and phishing email analysis

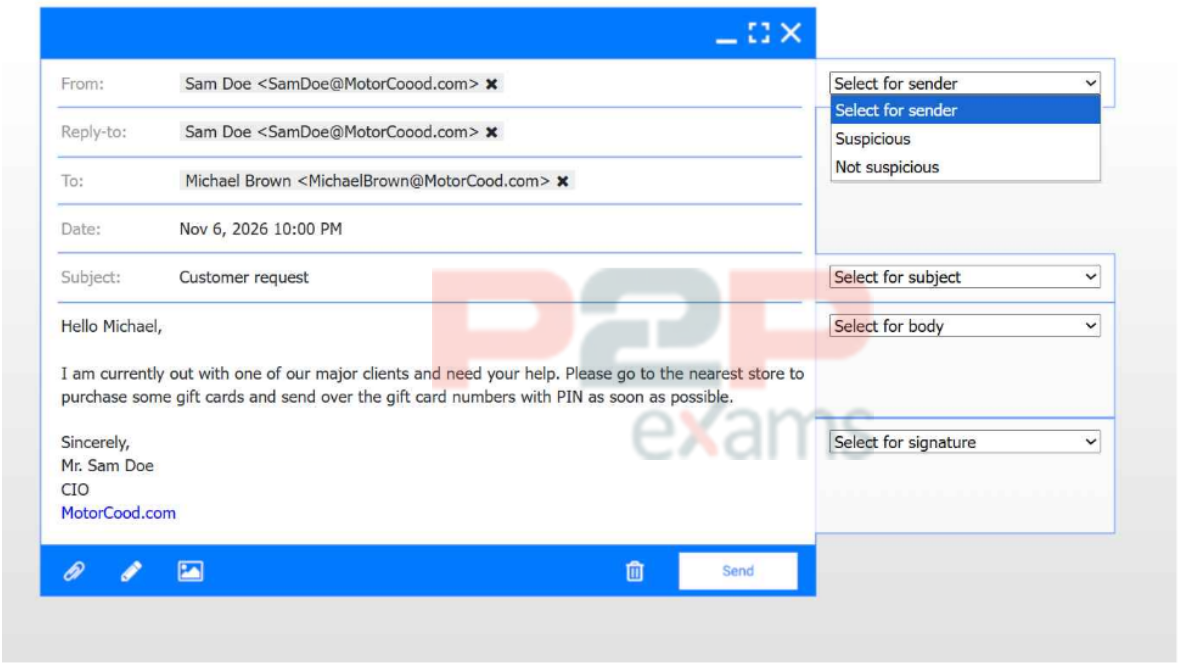
The CIO has reported that employees are receiving an email from someone claiming to be the

CIO and requesting a gift card be sent urgently via email.

As a security analyst, you have been assigned to investigate the email message and identify suspicious elements that could indicate a social engineering attack.

INSTRUCTIONS: Examine the email message and use the drop-down menus to determine whether each section is suspicious or not. If at any time you would like to return to the initial state of the simulation, click the Reset All button. In this printed version, clear your selections manually.





Field	Value
From	Sam Doe <SamDoe@MotorCoood.com>
Reply-to	Sam Doe <SamDoe@MotorCoood.com>
To	Michael Brown <MichaelBrown@MotorCood.com>
Date	Nov 6, 2026 10:00 PM
Subject	Customer request

Hello Michael,

I am currently out with one of our major clients and need your help. Please go to the nearest store to purchase some gift cards and send over the gift card numbers with PIN as soon as possible.

Sincerely,

Mr. Sam Doe

CIO

MotorCood.com

Answer area --- Select the appropriate classification

Each drop-down contains the following options: Suspicious; Not suspicious.

Email component	Suspicious	Not suspicious
Sender	?	?
Subject	?	?
Body	?	?
Signature	?	?

Options:

A- See the Explanation for detailed Answer

Answer:

A

Explanation:

Step 1: Identify the suspicious sender address

Selection: Suspicious

The displayed sender name is Sam Doe, but the sender's domain differs from the organization's legitimate domain.

Attribute	Observed value
Sender domain	MotorCoood.com
Reply-to domain	MotorCoood.com
Recipient domain	MotorCood.com
Signature domain	MotorCood.com

The sender's domain contains an additional letter ''o''. This is an example of typosquatting and executive impersonation. The attacker uses a visually similar domain name to make the email appear legitimate.

The matching malicious reply-to address also directs any responses to the suspicious domain.

Step 2: Examine the email subject

Selection: Not suspicious

The subject line is: Customer request.

The subject is generic and does not independently contain malicious links, threats, credential requests, or obvious impersonation indicators.

Although generic subject lines can be used in phishing campaigns, the subject alone does not establish malicious activity.

Step 3: Examine the email body

Selection: Suspicious

The email body contains several social engineering indicators:

* An executive is apparently requesting an unusual financial transaction.

* The recipient is instructed to purchase gift cards.

* The attacker requests both gift card numbers and PINs.

* The phrase ''as soon as possible'' creates urgency.

* The reference to a major client provides a fabricated business justification.

* The request bypasses established procurement and financial approval procedures.

Gift card numbers and PINs allow the value of purchased cards to be redeemed without physical possession of the cards.

The message combines authority, urgency, impersonation, and financial fraud.

Step 4: Examine the email signature

Selection: Not suspicious

The signature contains the executive's apparent name, organizational position, and correctly spelled company domain.

However, a valid-looking signature does not authenticate the sender. An attacker can copy legitimate corporate signatures, job titles, and branding to increase credibility.

The signature should therefore be classified as not independently suspicious, while the overall email remains malicious.

Step 5: Complete the simulation

Email component	Correct selection
Sender	Suspicious
Subject	Not suspicious
Body	Suspicious
Signature	Not suspicious

Step 6: Recommended security response

The security analyst should quarantine the phishing message, search for additional recipients, block the confirmed malicious sender domain where appropriate, alert affected employees, and investigate whether anyone disclosed gift card details or other sensitive information.

Employees should independently verify unusual executive requests through an established communication channel rather than replying to the suspicious email.

Attack classification: Business email compromise-style impersonation, typosquatting, phishing, and financial social engineering.

Question 4

Question Type: MultipleChoice

Which of the following describes the requirement to keep an entity's data only in a specified location?

Options:

A- Data sovereignty
B- Data ownership
C- Data classification
D- Data scalability

Answer:

A

Explanation:

Data sovereignty concerns the legal and regulatory authority governing information according to applicable jurisdictions. Organizations must consider where information is stored, processed, transferred, and accessed to ensure compliance with relevant national laws, regulatory obligations, and contractual requirements.

For example, an organization handling regulated financial or government information may be required to use approved data centers within a particular country or geographical region. Cloud architecture decisions must account for these requirements when selecting storage regions, backup locations, replication configurations, disaster recovery environments, and third-party service providers.

Data ownership establishes accountability and responsibility for organizational information assets. Data classification determines information sensitivity and associated protection requirements. Data scalability describes the ability of data infrastructure to accommodate changing storage or processing requirements.

A more technically precise term for the geographical placement of information is data residency, while data localization describes requirements restricting data storage or processing to specified jurisdictions.

Nevertheless, because neither alternative appears among the provided answer choices, data sovereignty is the most appropriate available answer given its relationship to geographical restrictions and jurisdictional data protection requirements.

Topic 2, Performance Base Questions (PBQ)

Question 5

Question Type: MultipleChoice

Which of the following should an organization implement to address privacy concerns for a

website that collects personal information?

Options:

A- User opt-out
B- Browser history expiration
C- Cache-clearing option
D- Restricted cookies

Answer:

A

Explanation:

A user opt-out mechanism enables individuals to decline or withdraw participation in specified personal information collection, processing, sharing, or marketing activities. It supports privacy management by providing users with greater control over how their personal information is handled.

Organizations operating websites that collect personal information should implement transparent privacy notices, appropriate consent mechanisms, clearly defined processing purposes, and accessible mechanisms for exercising applicable privacy rights.

An opt-out mechanism may allow users to unsubscribe from marketing communications, reject optional tracking, object to certain processing activities, or prevent specified disclosures of their information to third parties.

Browser history expiration removes locally stored browsing records after a defined period but does not necessarily affect information retained by the website operator. A cache-clearing option removes temporary browser content without controlling server-side data collection. Restricted cookies can reduce certain tracking activities but do not address all methods of collecting personal information.

User opt-out provides the broadest privacy control among the available options. However, where applicable legislation requires prior consent, an opt-out mechanism alone is insufficient; an appropriate opt-in process must also be implemented.

Question 6

Question Type: MultipleChoice

A security administrator at a large company with standardized processes receives a request from an operations engineer for a major system migration. Which of the following should the administrator do first?

Options:

A- Implement the configuration immediately.
B- Submit the configuration to a change advisory board.
C- Recommend the configuration to an executive for approval.
D- Schedule the configuration for the next update cycle.

Answer:

B

Explanation:

A Change Advisory Board (CAB) provides structured oversight of proposed changes to organizational information systems, infrastructure, applications, and operational environments. Its responsibilities commonly include evaluating proposed changes, reviewing associated risks, assessing business impact, and coordinating appropriate authorization.

A major system migration can introduce substantial operational and security consequences, including service interruptions, configuration errors, integration failures, data integrity issues, and changes to existing security controls.

Submitting the proposed migration to the CAB ensures that the modification is reviewed through the organization's established change management process before implementation.

The review may consider technical dependencies, testing requirements, resource availability, stakeholder communications, maintenance windows, rollback procedures, and security implications.

Implementing the configuration immediately bypasses formal governance and may introduce uncontrolled operational risk. Seeking approval from an individual executive does not necessarily satisfy the organization's standardized change authorization process. Scheduling the change before appropriate assessment and approval may create premature implementation commitments.

Among the available options, submission to the CAB most appropriately initiates formal review and authorization of the proposed major system migration.

Question 7

Question Type: MultipleChoice

Which of the following tools is best for troubleshooting anomalous network behavior?

Options:

A- Firewall
B- NetFlow
C- Simple Network Management Protocol (SNMP)
D- Security Content Automation Protocol (SCAP)

Answer:

B

Explanation:

NetFlow is a network traffic monitoring technology that collects detailed metadata about communications traversing supported network infrastructure. Flow records typically identify source and destination IP addresses, transport-layer ports, protocols, transferred byte volumes, packet counts, and communication durations.

Network administrators and security analysts use NetFlow to establish normal traffic patterns and identify deviations that may indicate security incidents, configuration problems, unauthorized communications, or operational inefficiencies.

For example, unusually large outbound transfers may indicate possible data exfiltration, while repeated communications across numerous destination ports may indicate network reconnaissance. Unexpected traffic destinations or communication frequencies can also help identify compromised systems.

A firewall primarily enforces network traffic filtering policies and generates records concerning permitted or blocked communications. SNMP supports infrastructure monitoring by collecting device health, interface utilization, operational status, and performance information. SCAP provides standardized mechanisms for security configuration assessment and vulnerability evaluation.

Although SNMP is particularly useful for troubleshooting device performance, NetFlow provides greater visibility into actual communication patterns between network systems.

NetFlow is the strongest available answer when investigating anomalous network traffic behavior.

Question 8

Question Type: MultipleChoice

Multiple personal devices are connected to a company's local area network (LAN). Company policy prohibits personal devices on the LAN. Which of the following solutions should the company use to prevent this activity?

Options:

A- 802.1X
B- VPN
C- Captive portal
D- Layer 3 firewall

Answer:

A

Explanation:

IEEE 802.1X is a port-based network access control standard that requires connecting devices or users to satisfy authentication requirements before receiving authorized access to network resources.

An 802.1X deployment commonly consists of three components: a supplicant operating on the connecting device, an authenticator such as a network switch or wireless access point, and an authentication server, typically using Remote Authentication Dial-In User Service (RADIUS).

When a device attempts to connect, the authenticator restricts normal network access until authentication succeeds. Organizations can enforce corporate device requirements by using device certificates, managed-device identities, or integrated network access control policies.

Unauthorized personal devices that cannot satisfy the established authentication and authorization requirements may be denied access or assigned to an isolated remediation network.

A virtual private network provides protected communication channels rather than controlling physical LAN connections. A captive portal typically provides browser-based authentication, often for guest networks. A Layer 3 firewall filters traffic based on network-layer information but does not independently establish device eligibility at the switch port.

Properly configured 802.1X provides the most appropriate mechanism for enforcing corporate

device access restrictions.

Question 9

Question Type: MultipleChoice

A company provides monthly reports about automated teller machine (ATM) transactions to different banks and is concerned about the privacy of user data in the report. Which of the following techniques will most likely address this concern?

Options:

A- Filtering
B- Masking
C- Hashing
D- Encoding

Answer:

B

Explanation:

Data masking is a privacy protection technique that obscures sensitive information while preserving sufficient structure, context, and usability for authorized business purposes. Masking is particularly useful when organizations must share reports containing information that external recipients do not need to view in its original form.

In the ATM transaction reporting scenario, sensitive information may include customer account numbers, payment card numbers, personal identifiers, and other confidential financial details.

Data masking can replace selected characters with substitute values, conceal portions of account numbers, or transform sensitive fields into approved representations. This enables recipient banks to examine relevant transaction information without unnecessarily exposing confidential customer data.

Filtering removes selected information or records according to predefined criteria. Although filtering may support data minimization, it does not necessarily preserve the structure of sensitive fields.

Hashing produces a fixed-length digest primarily associated with integrity verification and certain pseudonymization applications. Encoding changes the representation of information without

inherently providing confidentiality.

Data masking directly addresses the requirement to protect sensitive customer information while maintaining the operational usefulness of shared transaction reports.

Question 10

Question Type: MultipleChoice

Which of the following uses base and temporal metrics to prioritize remediation?

Options:

A- Common Vulnerabilities and Exposures (CVE)
B- Common Platform Enumeration (CPE)
C- Common Vulnerability Scoring System (CVSS)
D- Common Weakness Enumeration (CWE)

Answer:

C

Explanation:

The Common Vulnerability Scoring System (CVSS) provides a standardized framework for communicating the technical severity of security vulnerabilities. Organizations use CVSS scores alongside business risk, asset criticality, exposure, and threat intelligence to prioritize remediation activities.

CVSS versions 3.0 and 3.1 organize scoring information into three principal metric groups: Base, Temporal, and Environmental.

Base metrics describe the intrinsic characteristics of a vulnerability, including exploitation prerequisites and potential effects on confidentiality, integrity, and availability. Temporal metrics account for conditions that may change over time, such as exploit code maturity, remediation availability, and confidence in vulnerability reports. Environmental metrics incorporate characteristics specific to the affected organization's technology environment.

CVE provides standardized identifiers for publicly disclosed vulnerabilities. CPE identifies technology products, platforms, and versions. CWE categorizes common software and hardware weakness types.

None of these alternatives provides the vulnerability severity scoring framework described in the question.

CVSS is therefore correct. However, version awareness is important because CVSS v4.0 replaces the Temporal metric group with Threat metrics and introduces Supplemental metrics.

Question 11

Question Type: MultipleChoice

Which of the following is best suited to monitor and control the outbound movement of sensitive file content?

Options:

A- Web application firewall (WAF)
B- Extended detection and response (XDR)
C- Endpoint detection and response (EDR)
D- Data loss prevention (DLP)

Answer:

D

Explanation:

Data loss prevention (DLP) solutions identify sensitive information and enforce organizational policies governing its storage, processing, sharing, and transmission. Their primary objective is to prevent unauthorized disclosure, accidental information leakage, and deliberate data exfiltration.

DLP technologies can inspect file contents, classification labels, sensitive information patterns, document fingerprints, and contextual attributes to determine whether an attempted transfer violates established security policies.

For example, a DLP policy may prevent employees from uploading confidential financial documents to unauthorized cloud storage services or transmitting files containing personally identifiable information through external email channels.

Depending on the implementation, DLP can block transfers, quarantine information, generate alerts, notify users, or require authorized exceptions before allowing restricted activities.

A web application firewall protects web applications against malicious HTTP-based requests. XDR

integrates detection and response capabilities across multiple security domains. EDR focuses primarily on endpoint threat detection, investigation, and response.

Although these technologies may provide visibility into suspicious file activity, DLP specifically evaluates sensitive information against data-handling policies and controls unauthorized outbound transfers.

Question 12

Question Type: MultipleChoice

Which of the following vulnerabilities has most likely never been seen before?

Options:

A- Zero-day
B- Unpatched system
C- Rogue device
D- Obsolete system

Answer:

A

Explanation:

A zero-day vulnerability is a security weakness that is previously unknown to the responsible vendor or relevant defenders, or for which an effective security fix has not been made available when the weakness is discovered or exploited.

Zero-day vulnerabilities present significant security challenges because organizations may not possess established detection signatures, vendor-provided patches, or comprehensive information concerning exploitation conditions.

Threat actors capable of discovering or acquiring zero-day exploits may target vulnerable software before organizations have an opportunity to deploy permanent corrective measures.

Defensive strategies against emerging vulnerabilities include defense in depth, behavioral monitoring, application isolation, least-privilege enforcement, network segmentation, exploit prevention technologies, and timely threat intelligence integration.

An unpatched system contains missing security updates and may therefore remain exposed to

previously identified vulnerabilities. A rogue device is an unauthorized device connected to organizational infrastructure. An obsolete system is an outdated technology that may no longer receive appropriate vendor support or security maintenance.

Although these conditions can introduce serious security risks, they do not inherently describe previously unknown vulnerabilities. Zero-day is the most appropriate classification among the available options.

P2P exams

P2P exams

To Get Premium Files for SY0-801 Visit
https://www.p2pexams.com/products/sy0-801

For More Free Questions Visit
https://www.p2pexams.com/comptia/pdf/sy0-801

