CAS-003.47q

Number: CAS-003
Passing Score: 800
Time Limit: 120 min
File Version: 1

Comptia CAS-003

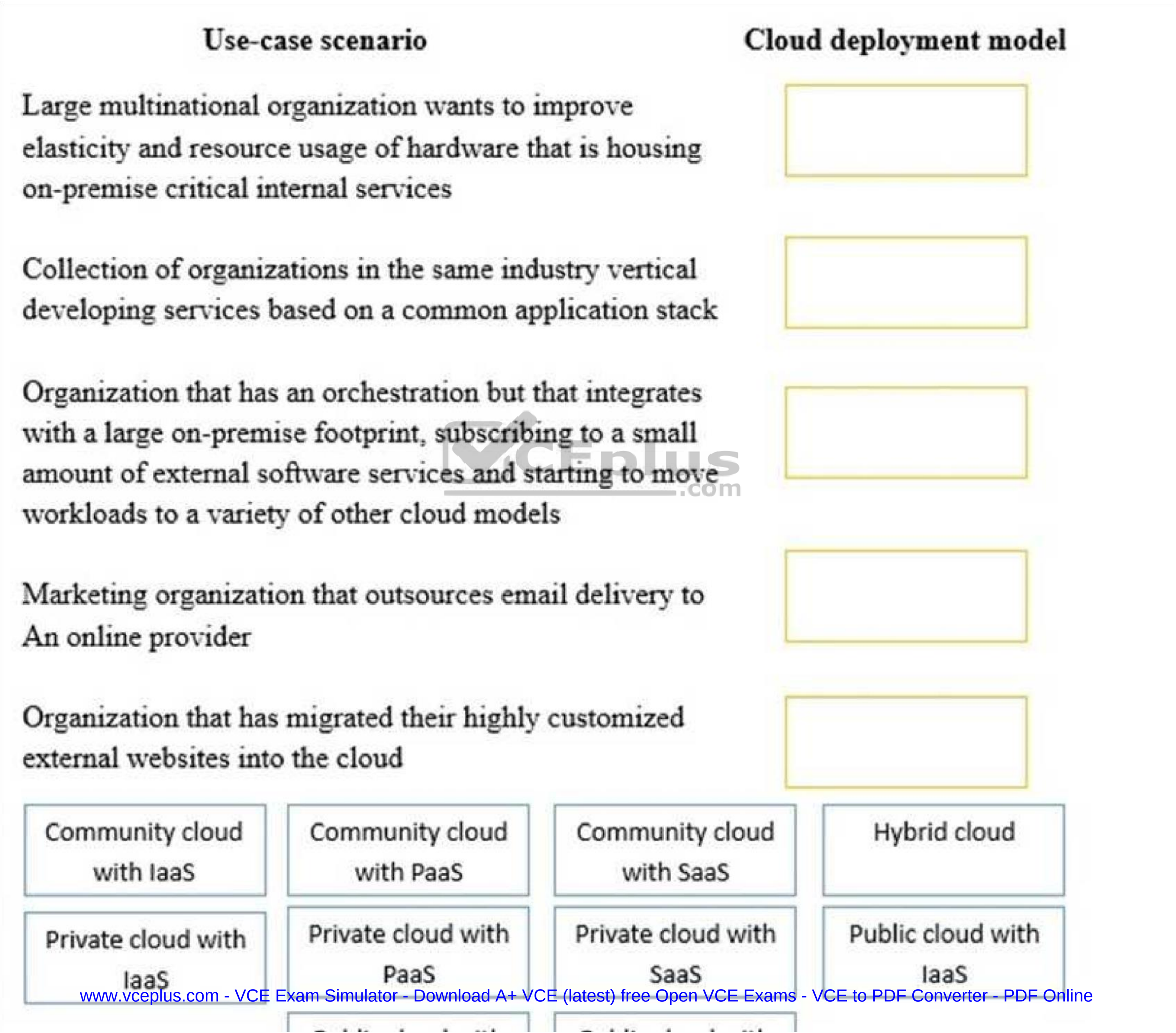
CompTIA Advanced Security Practitioner (CASP)

Exam C

QUESTION 1
DRAG DROP

Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.

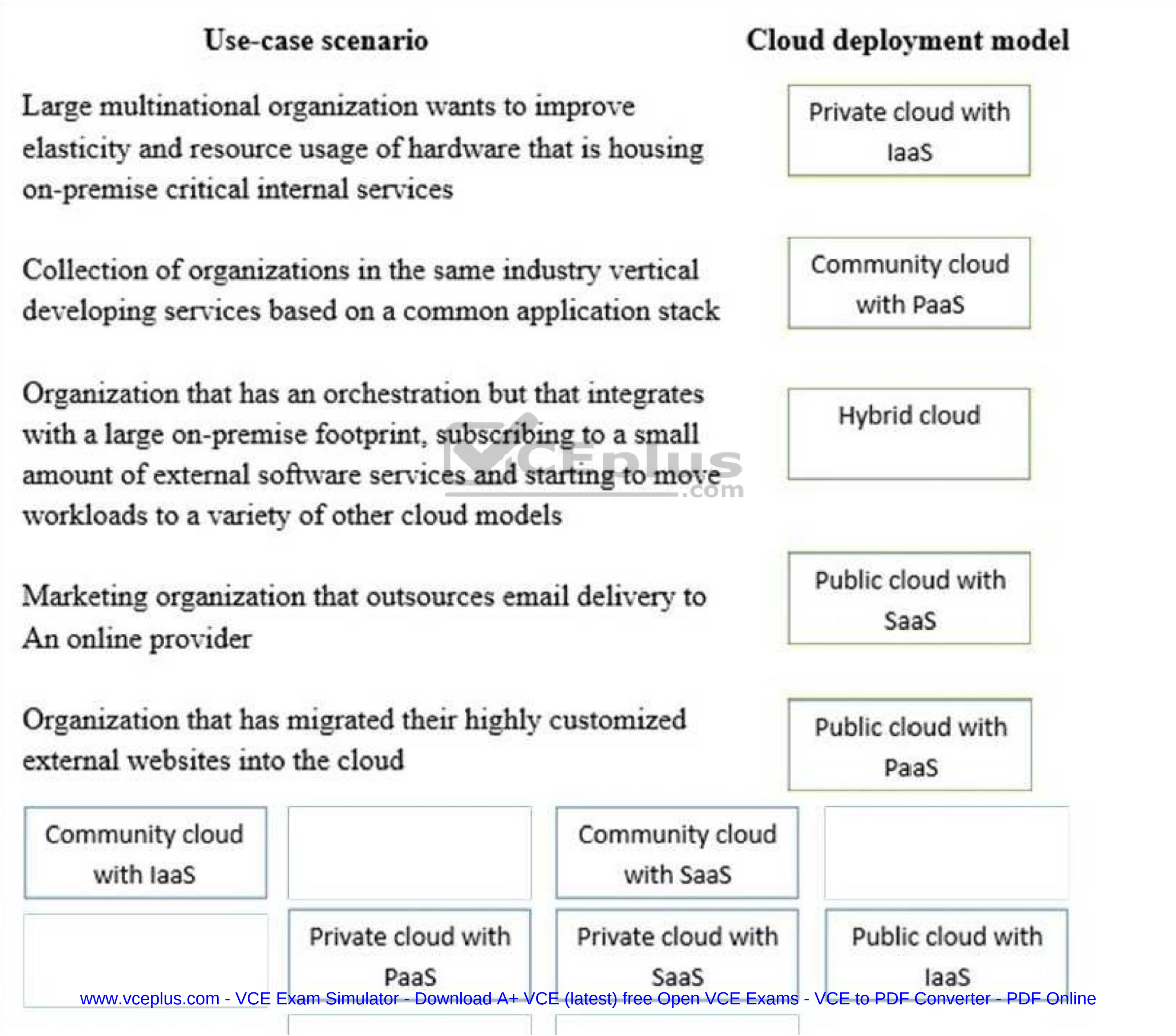
Select and Place:



Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	
Collection of organizations in the same industry vertical developing services based on a common application stack	
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	
Marketing organization that outsources email delivery to An online provider	
Organization that has migrated their highly customized external websites into the cloud	

Community cloud with IaaS	Community cloud with PaaS	Community cloud with SaaS	Hybrid cloud
Private cloud with IaaS	Private cloud with PaaS	Private cloud with SaaS	Public cloud with IaaS

Correct Answer:



Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS		Community cloud with SaaS	
	Private cloud with PaaS	Private cloud with SaaS	Public cloud with IaaS

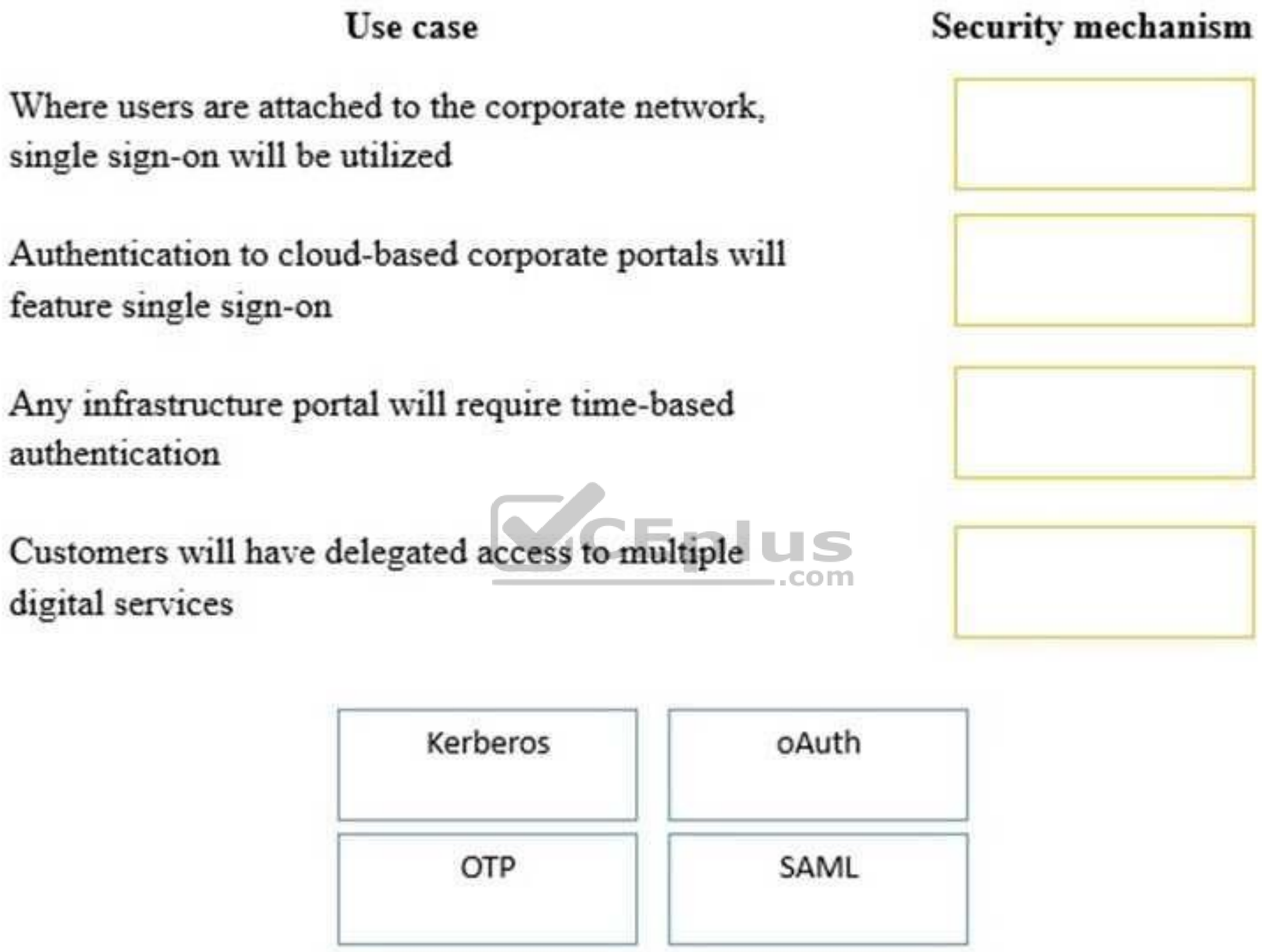
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
DRAG DROP

A security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once.

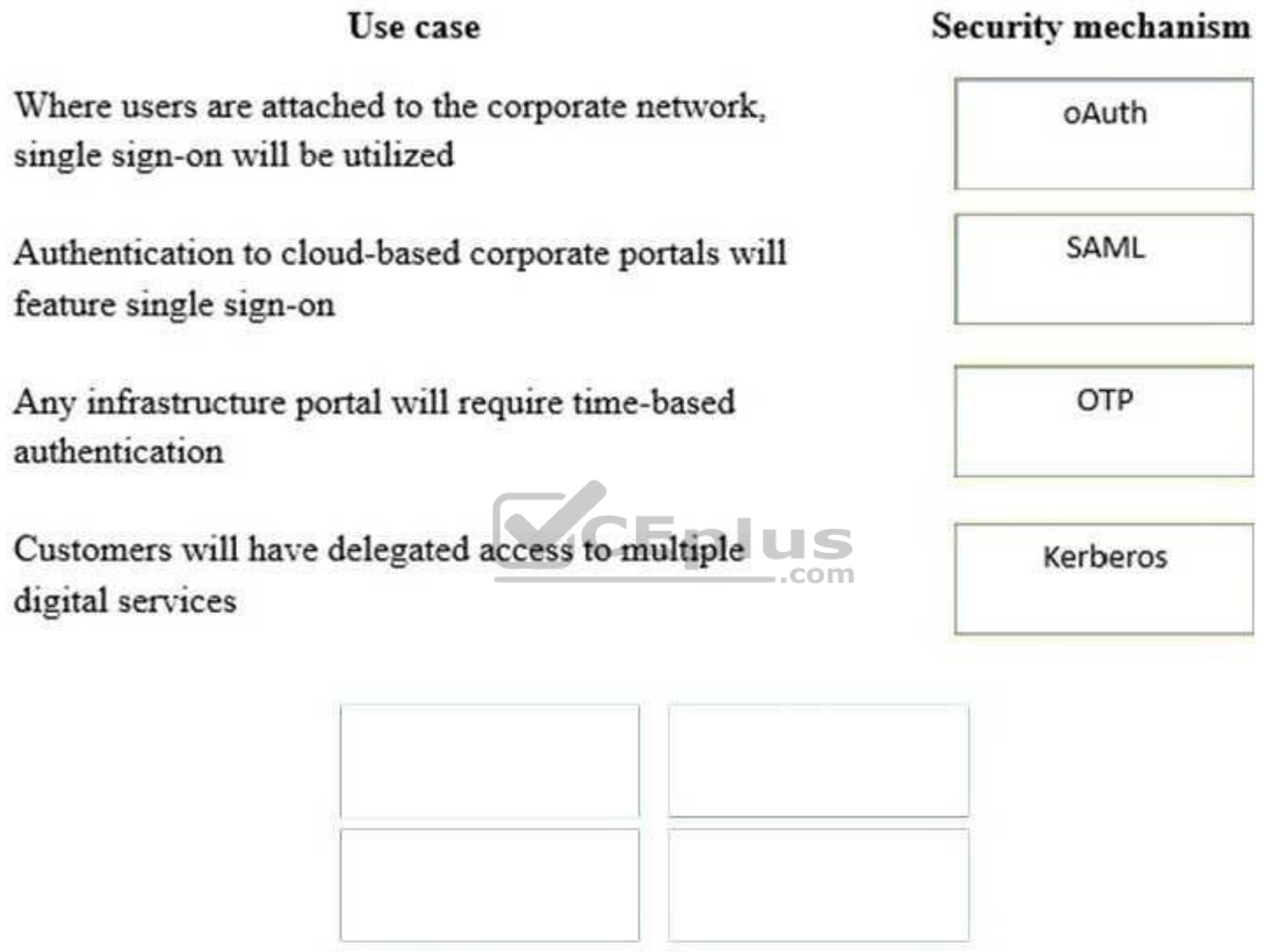
Select and Place:



Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

Kerberos	oAuth
OTP	SAML

Correct Answer:



Use case

Where users are attached to the corporate network, single sign-on will be utilized

Authentication to cloud-based corporate portals will feature single sign-on

Any infrastructure portal will require time-based authentication

Customers will have delegated access to multiple digital services

Security mechanism

oAuth

SAML

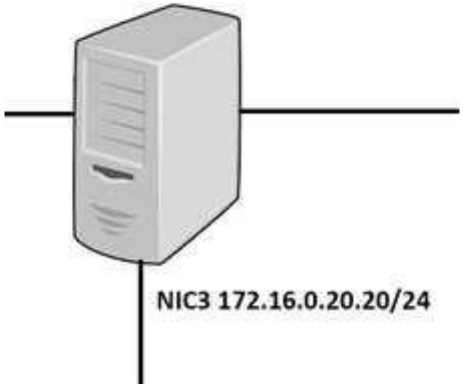
OTP

Kerberos

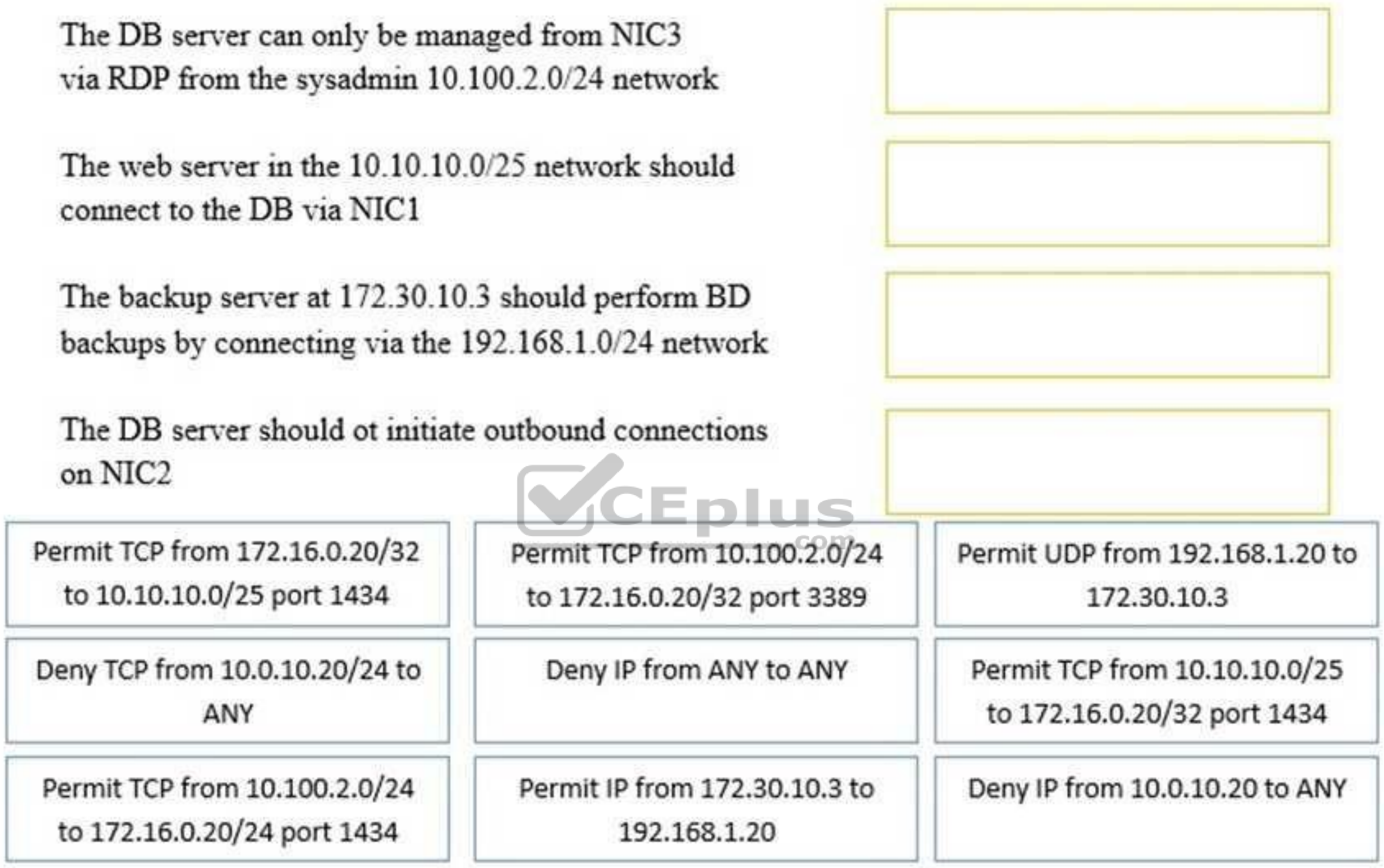
Section: (none)
Explanation
Explanation/Reference:

QUESTION 3
DRAG DROP

A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



Select and Place:



The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

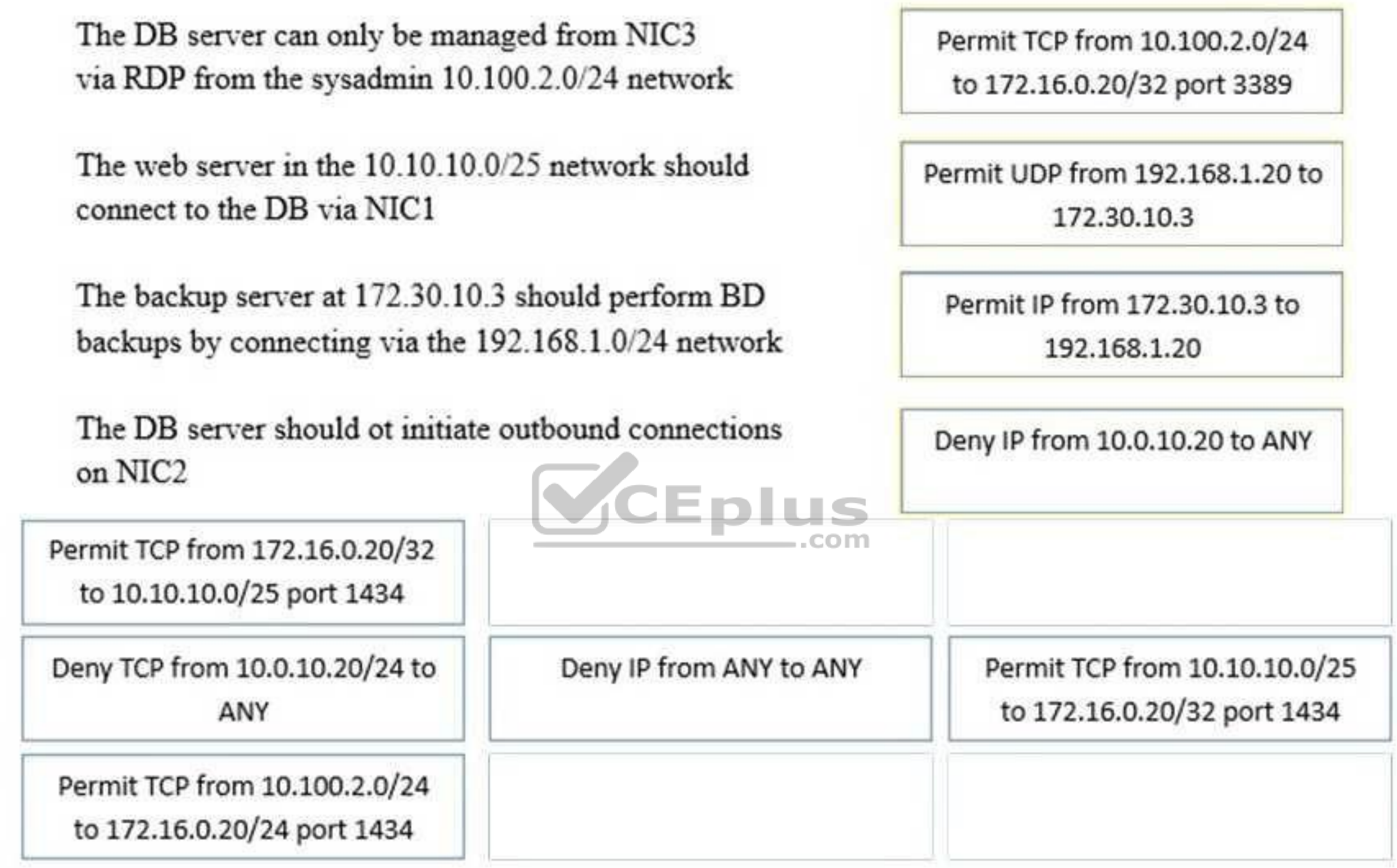
The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

The DB server should ot initiate outbound connections on NIC2

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434	Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389	Permit UDP from 192.168.1.20 to 172.30.10.3
Deny TCP from 10.0.10.20/24 to ANY	Deny IP from ANY to ANY	Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434	Permit IP from 172.30.10.3 to 192.168.1.20	Deny IP from 10.0.10.20 to ANY

Correct Answer:



The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

Permit UDP from 192.168.1.20 to 172.30.10.3

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

Permit IP from 172.30.10.3 to 192.168.1.20

The DB server should ot initiate outbound connections on NIC2

Deny IP from 10.0.10.20 to ANY

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434

Deny TCP from 10.0.10.20/24 to ANY

Deny IP from ANY to ANY

Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434

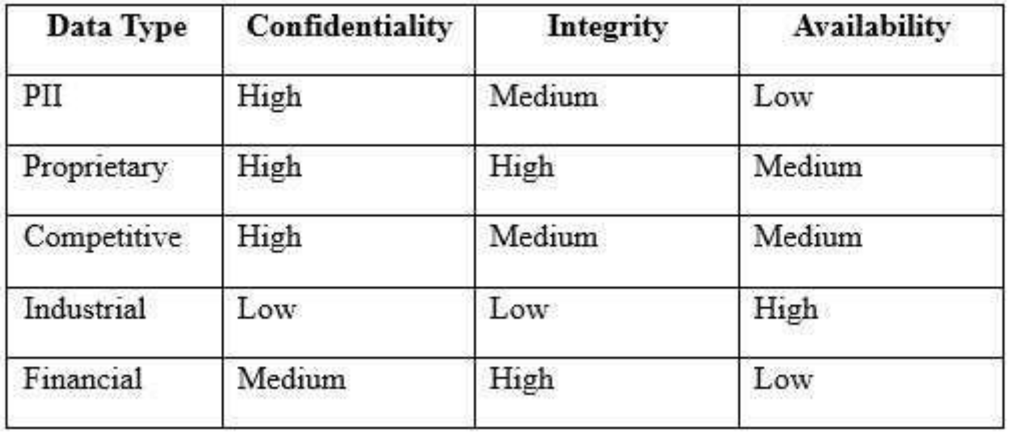
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434

Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.



Data Type	Confidentiality	Integrity	Availability
PII	High	Medium	Low
Proprietary	High	High	Medium
Competitive	High	Medium	Medium
Industrial	Low	Low	High
Financial	Medium	High	Low

Based on the data classification table above, which of the following BEST describes the overall classification?

A. High confidentiality, high availability
B. High confidentiality, medium availability
C. Low availability, low confidentiality
D. High integrity, low availability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

A. OTA updates

B. Remote wiping
C. Side loading
D. Sandboxing
E. Containerization
F. Signed applications

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software. The server was reimaged and patched offline. Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner
B. TPM
C. Host-based firewall
D. File integrity monitor
E. NIPS

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:

1. The ICS supplier has specified that any software installed will result in lack of support.
2. There is no documented trust boundary defined between the SCADA and corporate networks.
3. Operational technology staff have to manage the SCADA equipment via the engineering workstation.

4. There is a lack of understanding of what is within the SCADA network. Which of the following capabilities would BEST improve the security position?

A. VNC, router, and HIPS
B. SIEM, VPN, and firewall
C. Proxy, VPN, and WAF
D. IDS, NAC, and log monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

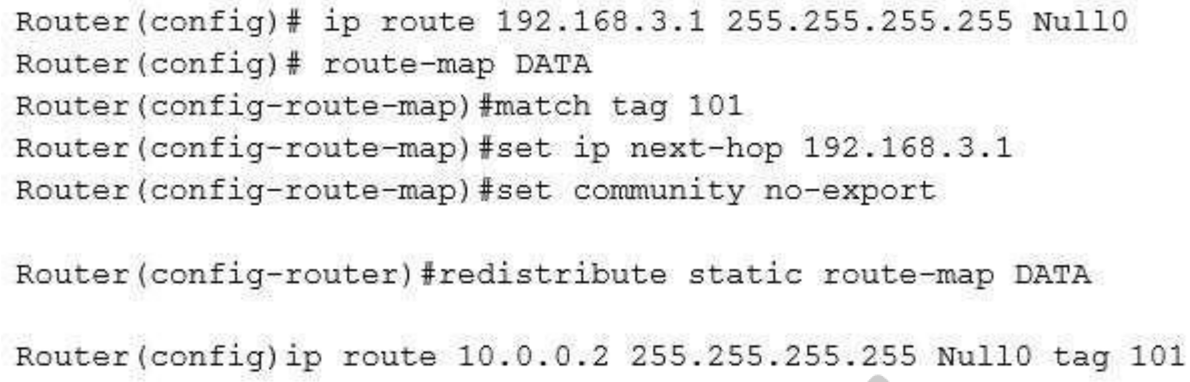
A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9

A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:



```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

Which of the following is the engineer implementing?

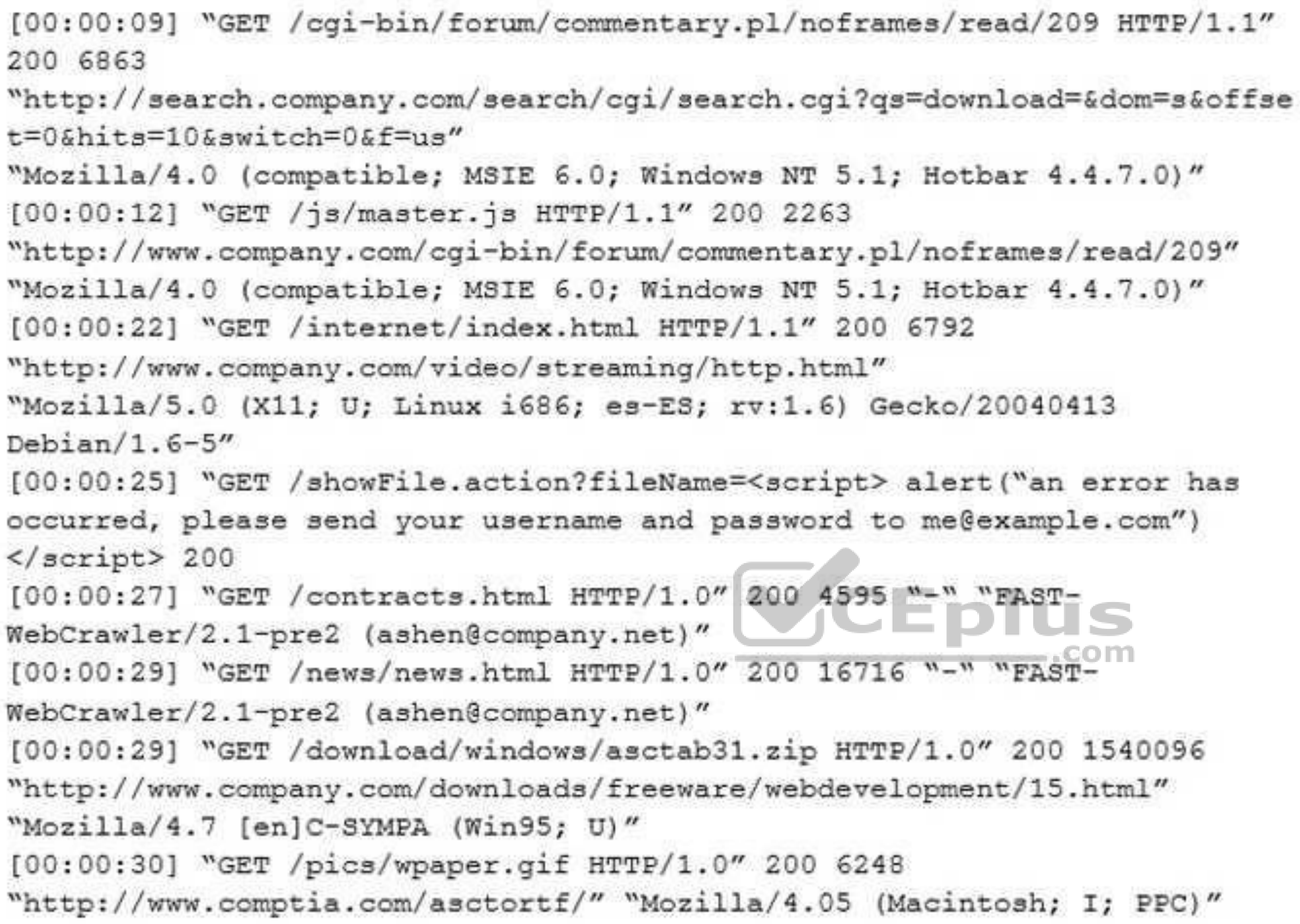
A. Remotely triggered black hole
B. Route protection
C. Port security
D. Transport security
E. Address space layout randomization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.



```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

A. SQLi
B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

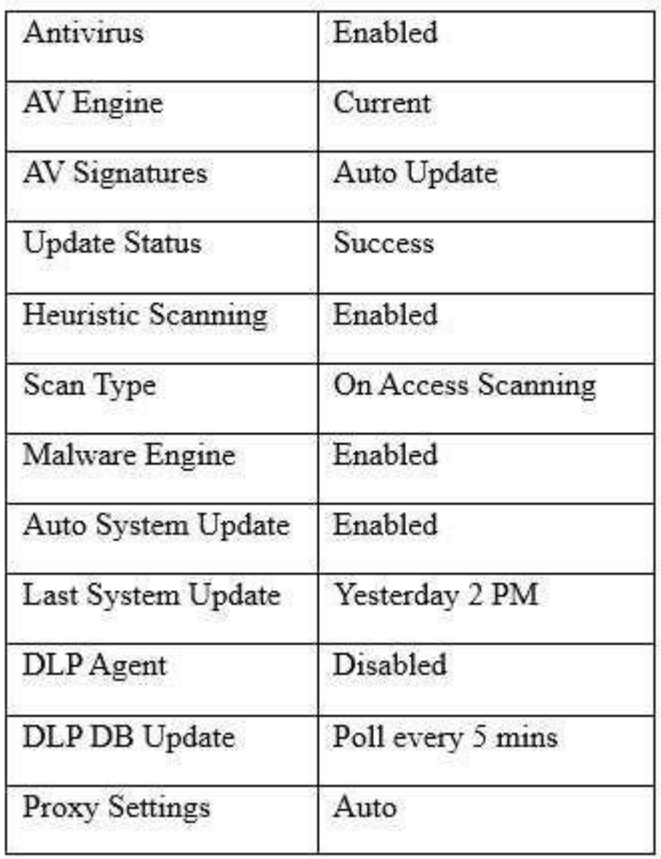
A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detection
D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:



Antivirus	Enabled
AV Engine	Current
AV Signatures	Auto Update
Update Status	Success
Heuristic Scanning	Enabled
Scan Type	On Access Scanning
Malware Engine	Enabled
Auto System Update	Enabled
Last System Update	Yesterday 2 PM
DLP Agent	Disabled
DLP DB Update	Poll every 5 mins
Proxy Settings	Auto

Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

A. Install HIPS
B. Enable DLP
C. Install EDR D. Install HIDS
E. Enable application blacklisting
F. Improve patch management processes

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

A. Deploy virtual desktop infrastructure with an OOB management network
B. Employ the use of vTPM with boot attestation
C. Leverage separate physical hardware for sensitive services and data
D. Use a community CSP with independently managed security services
E. Deploy to a private cloud with hosted hypervisors on each physical machine

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
- Duplicate IP addresses
- Rogue network devices
- Infected systems probing the company's network

Which of the following should be implemented to remediate the above issues? (Choose two.)

A. Port security
B. Route protection
C. NAC
D. HIPS
E. NIDS

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

A. Documentation of lessons learned
B. Quantitative risk assessment
C. Qualitative assessment of risk
D. Business impact scoring
E. Threat modeling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16

A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

A. Vulnerability assessment
B. Risk assessment
C. Patch management
D. Device quarantine
E. Incident management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A systems administrator at a medical imaging company discovers protected health information (PHI) on a general purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2
B. Immediately encrypt all PHI with AES 256
C. Delete all PHI from the network until the legal department is consulted
D. Consult the legal department to determine legal requirements

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 19

A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:

- High-impact controls implemented: 6 out of 10
- Medium-impact controls implemented: 409 out of 472
- Low-impact controls implemented: 97 out of 1000

The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:

- Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
- Average medium-impact control implementation cost: $6,250; Probable ALE for each medium-impact control gap: $11,000

Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

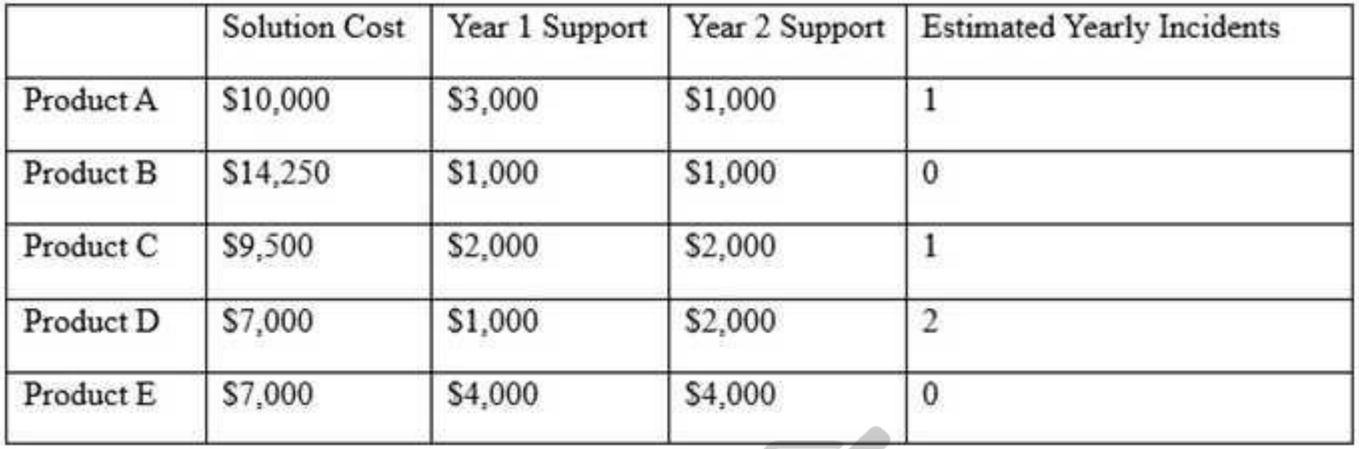
A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
B. The enterprise security team has focused exclusively on mitigating high-level risks
C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
D. The cybersecurity team has balanced residual risk for both high and medium controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:



	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	$10,000	$3,000	$1,000	1
Product B	$14,250	$1,000	$1,000	0
Product C	$9,500	$2,000	$2,000	1
Product D	$7,000	$1,000	$2,000	2
Product E	$7,000	$4,000	$4,000	0

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

A. Product A
B. Product B
C. Product C
D. Product D
E. Product E

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?

A. Update and deploy GPOs
B. Configure and use measured boot
C. Strengthen the password complexity requirements
D. Update the antivirus software and definitions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company’s client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

A. Install a HIPS on the web servers
B. Disable inbound traffic from offending sources
C. Disable SNMP on the web servers
D. Install anti-DDoS protection in the DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits

E. Continuous monitoring
F. Separation of duties

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

A. Magic link sent to an email address
B. Customer ID sent via push notification
C. SMS with OTP sent to a mobile number
D. Third-party social login
E. Certificate sent to be installed on a device

F. Hardware tokens sent to customers

Correct Answer: CE
Section: (none)
Explanation
Explanation/Reference:

QUESTION 26

A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

A. Review the CVE database for critical exploits over the past year
B. Use social media to contact industry analysts

C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. Perform a penetration test of the competitor’s network and share the results with the board

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO’s request?

A. 1. Perform the ongoing research of the best practices
2. Determine current vulnerabilities and threats
3. Apply Big Data techniques
4. Use antivirus control
B. 1. Apply artificial intelligence algorithms for detection
2. Inform the CERT team
3. Research threat intelligence and potential adversaries
4. Utilize threat intelligence to apply Big Data techniques
C. 1. Obtain the latest IOCs from the open source repositories
2. Perform a sweep across the network to identify positive matches
3. Sandbox any suspicious files
4. Notify the CERT team to apply a future proof threat model D. 1. Analyze the current threat intelligence
2. Utilize information sharing to obtain the latest industry IOCs
3. Perform a sweep across the network to identify positive matches
4. Apply machine learning algorithms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29

A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

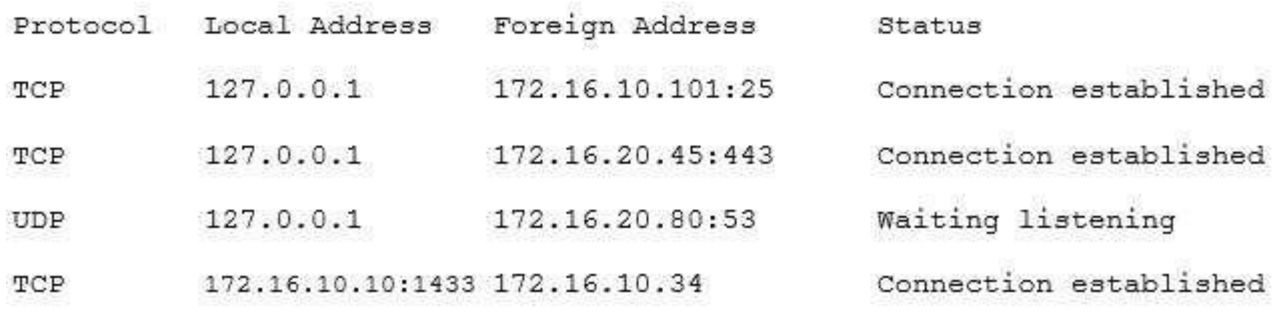
A. Restrict access to the network share by adding a group only for developers to the share's ACL
B. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory services
C. Obfuscate the username within the script file with encoding to prevent easy identification and the account used
D. Provision a new user account within the enterprise directory and enable its use for authentication to the target applications. Share the username and password with all developers for use in their individual scripts
E. Redesign the web applications to accept single-use, local account credentials for authentication

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30

A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:



```
Protocol    Local Address        Foreign Address        Status
TCP         127.0.0.1            172.16.10.101:25       Connection established
TCP         127.0.0.1            172.16.20.45:443       Connection established
UDP         127.0.0.1            172.16.20.80:53        Waiting listening
TCP         172.16.10.10:1433    172.16.10.34           Connection established
```

Which of the following commands would have provided this output?

A. `arp -s`

B. `netstat -a`

C. `ifconfig -arp`

D. `sqlmap -w`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

Management is reviewing the results of a recent risk assessment of the organization’s policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

A. Transfer

B. Mitigate

C. Accept

D. Avoid

E. Reject

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

```
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
```

Which of the following did the analyst use to determine the location of the malicious payload?

A. Code deduplicators
B. Binary reverse-engineering
C. Fuzz testing
D. Security containers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33

A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

A. Issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME
B. Federate with an existing PKI provider, and reject all non-signed emails
C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34

Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 35

Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

A. Business partnership agreement
B. Memorandum of understanding
C. Service-level agreement
D. Interconnection security agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-47.pdf

QUESTION 36

A company is developing requirements for a customized OS build that will be used in an embedded environment. The company procured hardware that is capable of reducing the likelihood of successful buffer overruns while executables are processing. Which of the following capabilities must be included for the OS to take advantage of this critical hardware-based countermeasure?

A. Application whitelisting
B. NX/XN bit
C. ASLR
D. TrustZone
E. SCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development. Which of the following SDLC best practices should the development team have followed?

A. Implementing regression testing
B. Completing user acceptance testing
C. Verifying system design documentation
D. Using a SRTM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38

An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations
B. Configure the devices to use an always-on IPSec VPN
C. Configure all management traffic to be tunneled into the enterprise via TLS
D. Implement a VDI solution and deploy supporting client apps to devices
E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Correct Answer: BE
Section: (none)
Explanation
Explanation/Reference:

QUESTION 39

After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases: ▪ Selection of a cloud provider

- Architectural design
- Microservice segmentation
- Virtual private cloud
- Geographic service redundancy
- Service migration

The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

A. Multicloud solution
B. Single-tenancy private cloud
C. Hybrid cloud solution
D. Cloud access security broker

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: "`<object object_ref=… />`" and "`<state state_ref=… />`". Which of the following tools BEST supports the use of these definitions?

A. HTTP interceptor
B. Static code analyzer
C. SCAP scanner
D. XML fuzzer

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 41
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization:

```
localStorage.setItem("session-cookie", document.cookie);
```

Which of the following should the security engineer recommend?

A. SessionStorage should be used so authorized cookies expire after the session ends
B. Cookies should be marked as "secure" and "HttpOnly"
C. Cookies should be scoped to a relevant domain/path
D. Client-side cookies should be replaced by server-side mechanisms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 43

A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer
(CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed

E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A deployment manager is working with a software development group to assess the security of a new version of the organization's internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

A. Static code analysis in the IDE environment
B. Penetration testing of the UAT environment
C. Vulnerability scanning of the production environment
D. Penetration testing of the production environment
E. Peer review prior to unit testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
During a security event investigation, a junior analyst fails to create an image of a server's hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

A. Continuity of operations
B. Chain of custody
C. Order of volatility
D. Data recovery

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.computer-forensics-recruiter.com/order-of-volatility/

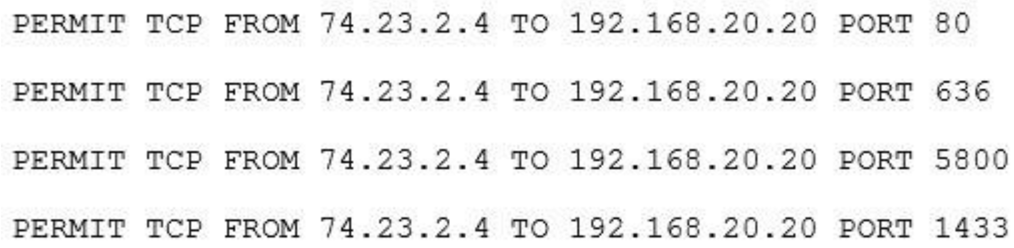
QUESTION 46
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (CIO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS
B. Hybrid IaaS
C. Single-tenancy PaaS
D. Community IaaS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a thirdparty service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:



```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

A. LDAP
B. WAYF
C. OpenID
D. RADIUS
E. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: