

➤ **Vendor:** CompTIA

➤ **Exam Code:** SY0-601

➤ **Exam Name:** Microsoft Azure Architect Technologies

➤ **New Updated Questions from** [Braindump2go](#) (**Updated in** [Nov./2020](#))

Visit Braindump2go and Download Full Version SY0-601 Exam Dumps

Exam A

QUESTION 1 SIMULATION

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

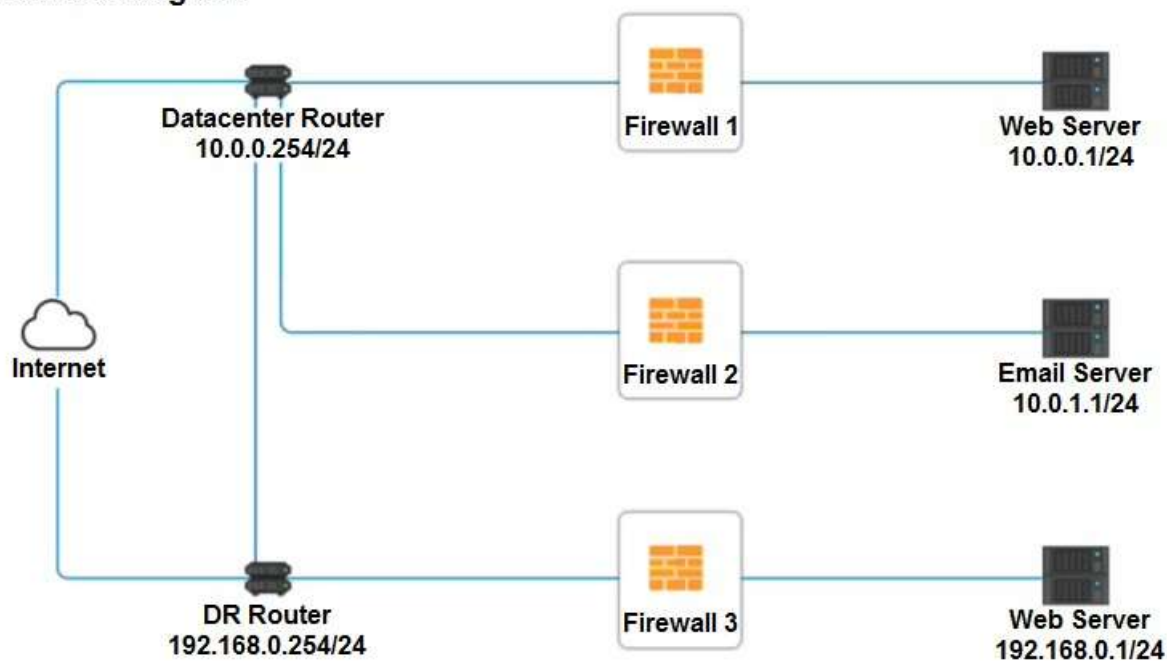
Click on each firewall to do the following:

1. Deny cleartext web traffic.
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

Network Diagram



Firewall 1
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
Management	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>

Reset Answer
Save
Close

Firewall 2
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
Management	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>

Reset Answer
Save
Close

Firewall 3
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTPS Outbound	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
Management	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTPS Inbound	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>
HTTP Inbound	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div>PERMIT DENY</div> </div>

Reset Answer
Save
Close

Correct Answer: See explanation below.

QUESTION 2

DRAG DROP

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

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

Select and Place:

Commands

chmod 644 ~/.ssh/id_rsa

chmod 777 ~/.ssh/authorized_keys

ssh-keygen -t rsa

scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys

ssh-copy-id -i ~/.ssh/id_rsa.pub user@server

ssh -i ~/.ssh/id_rsa user@server

ssh root@server

SSH Client

Correct Answer:

Commands

chmod 644 ~/.ssh/id_rsa

chmod 777 ~/.ssh/authorized_keys

ssh-keygen -t rsa

scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys

ssh-copy-id -i ~/.ssh/id_rsa.pub user@server

ssh -i ~/.ssh/id_rsa user@server

ssh root@server

SSH Client

ssh-keygen -t rsa

ssh-copy-id -i ~/.ssh/id_rsa.pub user@server

chmod 644 ~/.ssh/id_rsa

ssh root@server

QUESTION 3

HOTSPOT

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

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

Hot Area:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div>	<div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div>
The attack establishes a connection, which allows remote commands to be executed.	User	<div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div>	<div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div>
The attack is self propagating and compromises a SQL database using well known credentials as it moves through the network.	Database server	<div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div>	<div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div>	<div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div>
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div>	<div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div>

Correct Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well known credentials as it moves through the network.	Database server	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

QUESTION 4

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human- management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption
- E. SQL injection
- F. Server-side request forgery

Correct Answer: DF

QUESTION 5

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

Correct Answer: C

QUESTION 6

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Correct Answer: D

QUESTION 7

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map

- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

Correct Answer: AC

QUESTION 8

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

Correct Answer: A

QUESTION 9

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Correct Answer: C

QUESTION 10

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Correct Answer: C

QUESTION 11

On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

- A. Data accessibility
- B. Legal hold
- C. Cryptographic or hash algorithm
- D. Data retention legislation
- E. Value and volatility of data
- F. Right-to-audit clauses

Correct Answer: EF

QUESTION 12

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

Correct Answer: B

QUESTION 13

A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

Correct Answer: B