

CompTIA SY0-701 Questions & Answers



Security+ (Plus) Certification

Version: 7.0

QUESTION NO: 1

Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

- A.**
Hactivist
- B.**
Whistleblower
- C.**
Organized crime
- D.**
Unskilled attacker

Answer: C

QUESTION NO: 2

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

- A.**
Key stretching
- B.**
Data masking
- C.**
Steganography
- D.**
Salting

Answer: D

QUESTION NO: 3

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found?"

error message. Which of the following types of social engineering attacks occurred?

- A.**
Brand impersonation
- B.**
Pretexting
- C.**
Typosquatting
- D.**
Phishing

Answer: D

QUESTION NO: 4

An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

- A.**

Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53

Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
- B.**

Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
- C.**

Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
- D.**

Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Answer: C

QUESTION NO: 5

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

- A.**
SSO
- B.**
LEAP
- C.**
MFA
- D.**
PEAP

Answer: A

QUESTION NO: 6

Which of the following scenarios describes a possible business email compromise attack?

- A.**
An employee receives a gift card request in an email that has an executive's name in the display field of the email.
- B.**
Employees who open an email attachment receive messages demanding payment in order to access files.
- C.**
A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
- D.**
An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Answer: A

QUESTION NO: 7

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

- A.**
Jump server
- B.**
RADIUS
- C.**
HSM
- D.**
Load balancer

Answer: A

QUESTION NO: 8

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to **best** protect against similar attacks in the future?

- A.**
NGFW
- B.**
WAF
- C.**
TLS
- D.**
SD-WAN

Answer: B

QUESTION NO: 9

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

- A.**
Multifactor authentication
- B.**
Permissions assignment
- C.**
Access management
- D.**
Password complexity

Answer: A

QUESTION NO: 10

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

- A.**
Typosquatting
- B.**
Phishing
- C.**
Impersonation
- D.**
Vishing
- E.**
Smishing
- F.**
Misinformation

Answer: C,E

QUESTION NO: 11

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:

"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address.?"

Which of the following are the **best** responses to this situation? (Choose two).

- A.**
Cancel current employee recognition gift cards.
- B.**
Add a smishing exercise to the annual company training.
- C.**
Issue a general email warning to the company.
- D.**
Have the CEO change phone numbers.
- E.**
Conduct a forensic investigation on the CEO's phone.
- F.**
Implement mobile device management.

Answer: B,C

QUESTION NO: 12

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A.**
A thorough analysis of the supply chain
- B.**
A legally enforceable corporate acquisition policy

C.

A right to audit clause in vendor contracts and SOWs

D.

An in-depth penetration test of all suppliers and vendors

Answer: A

QUESTION NO: 13

Which of the following provides the details about the terms of a test with a third-party penetration tester?

A.

Rules of engagement

B.

Supply chain analysis

C.

Right to audit clause

D.

Due diligence

Answer: A

QUESTION NO: 14

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A.

Active

B.

Passive

C.

Defensive

D.

Offensive

Answer: A

QUESTION NO: 15

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A.**
IRP
- B.**
DRP
- C.**
RPO
- D.**
SDLC

Answer: B

QUESTION NO: 16

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A.**
Jailbreaking
- B.**
Memory injection
- C.**
Resource reuse
- D.**
Side loading

Answer: D

QUESTION NO: 17

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is **most** likely occurring?

- A.**
Password spraying
- B.**
Account forgery
- C.**
Pass-the-hash
- D.**
Brute-force

Answer: A

QUESTION NO: 18

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be **most** relevant for the analyst to evaluate?

- A.**
Secured zones
- B.**
Subject role
- C.**
Adaptive identity
- D.**
Threat scope reduction

Answer: A

QUESTION NO: 19

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the **best** solution?

- A.**
RDP server
- B.**
Jump server
- C.**
Proxy server
- D.**
Hypervisor

Answer: B

QUESTION NO: 20

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A.**
encryption=off
- B.**
http://
- C.**
www.*.com
- D.**
:443

Answer: B

QUESTION NO: 21

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

- A.
access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
- B.
access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
- C.
access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
- D.
access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

QUESTION NO: 22

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is **most** secure?

- A.
Implementing a bastion host
- B.
Deploying a perimeter network
- C.
Installing a WAF
- D.
Utilizing single sign-on

Answer: A

QUESTION NO: 23

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic

coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

- A.
Application
- B.
IPS/IDS
- C.
Network
- D.
Endpoint

Answer: D

QUESTION NO: 24

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.

SIEM alerts have not yet been configured. Which of the following **best** describes what the security analyst should do to identify this behavior?

- A.
Digital forensics
- B.
E-discovery
- C.
Incident response
- D.
Threat hunting

Answer: D

QUESTION NO: 25

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

- A.**
Accept
- B.**
Transfer
- C.**
Mitigate
- D.**
Avoid

Answer: B

QUESTION NO: 26

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

- A.**
Partition
- B.**
Asymmetric
- C.**
Full disk
- D.**
Database

Answer: C

QUESTION NO: 27

Which of the following security control types does an acceptable use policy **best** represent?

- A.**
Detective

- B.**
Compensating
- C.**
Corrective
- D.**
Preventive

Answer: D

QUESTION NO: 28

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

- A.**
Hardening
- B.**
Employee monitoring
- C.**
Configuration enforcement
- D.**
Least privilege

Answer: D

QUESTION NO: 29

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

- A.**
Risk tolerance
- B.**
Risk transfer
- C.**

Risk register

D.

Risk analysis

Answer: C

QUESTION NO: 30

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

A.

Disaster recovery plan

B.

Incident response procedure

C.

Business continuity plan

D.

Change management procedure

Answer: D

QUESTION NO: 31

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following **best** describes the program the company is setting up?

A.

Open-source intelligence

B.

Bug bounty

C.

Red team

D.

Penetration testing

Answer: B

QUESTION NO: 32

Which of the following threat actors is the **most** likely to use large financial resources to attack critical systems located in other countries?

- A.**
Insider
- B.**
Unskilled attacker
- C.**
Nation-state
- D.**
Hacktivist

Answer: C

QUESTION NO: 33

Which of the following enables the use of an input field to run commands that can view or manipulate data?

- A.**
Cross-site scripting
- B.**
Side loading
- C.**
Buffer overflow
- D.**
SQL injection

Answer: D

QUESTION NO: 34

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are **most** likely to use in day-to-day work activities?

- A.**
Encrypted
- B.**
Intellectual property
- C.**
Critical
- D.**
Data in transit

Answer: B

QUESTION NO: 35

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

- A.**
If a security incident occurs on the device, the correct employee can be notified.
- B.**
The security team will be able to send user awareness training to the appropriate device.
- C.**
Users can be mapped to their devices when configuring software MFA tokens.
- D.**
User-based firewall policies can be correctly targeted to the appropriate laptops.
- E.**
When conducting penetration testing, the security team will be able to target the desired laptops.
- F.**
Company data can be accounted for when the employee leaves the organization.

Answer: A,F

QUESTION NO: 36

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the **best** option?

- A.**
Send out periodic security reminders.
- B.**
Update the content of new hire documentation.
- C.**
Modify the content of recurring training.
- D.**
Implement a phishing campaign.

Answer: C

QUESTION NO: 37

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

- A.**
Packet captures
- B.**
Vulnerability scans
- C.**
Metadata
- D.**
Dashboard

Answer: D

QUESTION NO: 38

A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following **most** likely occurred?

- A.**
The end user changed the file permissions.
- B.**
A cryptographic collision was detected.
- C.**
A snapshot of the file system was taken.
- D.**
A rootkit was deployed.

Answer: D

QUESTION NO: 39

Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

- A.**
Client
- B.**
Third-party vendor
- C.**
Cloud provider
- D.**
DBA

Answer: A

QUESTION NO: 40

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

- A.
MSA
- B.
SLA
- C.
BPA
- D.
SOW

Answer: D

QUESTION NO: 41

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

- A.
Secure cookies
- B.
Version control
- C.
Input validation
- D.
Code signing

Answer: C

QUESTION NO: 42

Which of the following must be considered when designing a high-availability network? (Choose two).

- A.**
Ease of recovery
- B.**
Ability to patch
- C.**
Physical isolation
- D.**
Responsiveness
- E.**
Attack surface
- F.**
Extensible authentication

Answer: A,D

QUESTION NO: 43

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken **first**?

- A.**
Air gap the system.
- B.**
Move the system to a different network segment.
- C.**
Create a change control request.
- D.**
Apply the patch to the system.

Answer: C

QUESTION NO: 44

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

- A.**
To gather IoCs for the investigation
- B.**
To discover which systems have been affected
- C.**
To eradicate any trace of malware on the network
- D.**
To prevent future incidents of the same nature

Answer: D

QUESTION NO: 45

Which of the following is the **most** likely outcome if a large bank fails an internal PCI DSS compliance assessment?

- A.**
Fines
- B.**
Audit findings
- C.**
Sanctions
- D.**
Reputation damage

Answer: A

QUESTION NO: 46

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following **best** describes this step?

- A.**
Capacity planning
- B.**

Redundancy

C.

Geographic dispersion

D.

Tabletop exercise

Answer: A

QUESTION NO: 47

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the **most** effective way to limit this access?

A.

Data masking

B.

Encryption

C.

Geolocation policy

D.

Data sovereignty regulation

Answer: C

QUESTION NO: 48

Which of the following is a hardware-specific vulnerability?

A.

Firmware version

B.

Buffer overflow

C.

SQL injection

D.
Cross-site scripting

Answer: A

QUESTION NO: 49

While troubleshooting a firewall configuration, a technician determines that a “deny any?” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.

Which of the following actions would prevent this issue?

- A.**
Documenting the new policy in a change request and submitting the request to change management
- B.**
Testing the policy in a non-production environment before enabling the policy in the production network
- C.**
Disabling any intrusion prevention signatures on the “deny any?” policy prior to enabling the new policy
- D.**
Including an “allow any?” policy above the “deny any?” policy

Answer: B

QUESTION NO: 50

An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the **best** for this scenario?

- A.**
Real-time recovery
- B.**
Hot

C.

Cold

D.

Warm

Answer: C

QUESTION NO: 51

A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following **best** describes this policy?

A.

Enumeration

B.

Sanitization

C.

Destruction

D.

Inventory

Answer: B

QUESTION NO: 52

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A.

Private

B.

Critical

C.

Sensitive

D.

Public

Answer: C

QUESTION NO: 53

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider **first**?

- A.**
Local data protection regulations
- B.**
Risks from hackers residing in other countries
- C.**
Impacts to existing contractual obligations
- D.**
Time zone differences in log correlation

Answer: A

QUESTION NO: 54

Which of the following would be the **best** way to block unknown programs from executing?

- A.**
Access control list
- B.**
Application allow list
- C.**
Host-based firewall
- D.**
DLP solution

Answer: B

QUESTION NO: 55

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.

Which of the following teams will conduct this assessment activity?

- A.
White
- B.
Purple
- C.
Blue
- D.
Red

Answer: D

QUESTION NO: 56

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the **most** appropriate?

- A.
Testing input validation on the user input fields
- B.
Performing code signing on company-developed software
- C.
Performing static code analysis on the software
- D.
Ensuring secure cookies are use

Answer: B

QUESTION NO: 57

Which of the following can be used to identify potential attacker activities without affecting production servers?

- A.**
Honeypot
- B.**
Video surveillance
- C.**
Zero Trust
- D.**
Geofencing

Answer: A

QUESTION NO: 58

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

- A.**
Analysis
- B.**
Lessons learned
- C.**
Detection
- D.**
Containment

Answer: A

QUESTION NO: 59

A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done **next**?

- A.**
Conduct an audit.
- B.**

Initiate a penetration test.

C.

Rescan the network.

D.

Submit a report.

Answer: C

QUESTION NO: 60

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following **best** describes the user's activity?

A.

Penetration testing

B.

Phishing campaign

C.

External audit

D.

Insider threat

Answer: D

QUESTION NO: 61

Which of the following allows for the attribution of messages to individuals?

A.

Adaptive identity

B.

Non-repudiation

C.

Authentication

D.
Access logs

Answer: B

QUESTION NO: 62

Which of the following is the **best** way to consistently determine on a daily basis whether security settings on servers have been modified?

- A.**
Automation
- B.**
Compliance checklist
- C.**
Attestation
- D.**
Manual audit

Answer: A

QUESTION NO: 63

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A.**
SCAP
- B.**
NetFlow
- C.**
Antivirus
- D.**
DLP

Answer: D

QUESTION NO: 64

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, ;, &, `, and ? from variables set by forms in a web application.

Which of the following **best** explains the security technique the organization adopted by making this addition to the policy?

- A.**
Identify embedded keys
- B.**
Code debugging
- C.**
Input validation
- D.**
Static code analysis

Answer: C

QUESTION NO: 65

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

- A.**
Place posters around the office to raise awareness of common phishing activities.
- B.**
Implement email security filters to prevent phishing emails from being delivered.
- C.**
Update the EDR policies to block automatic execution of downloaded programs.
- D.**
Create additional training for users to recognize the signs of phishing attempts.

Answer: C

QUESTION NO: 66

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A.**
Compensating control
- B.**
Network segmentation
- C.**
Transfer of risk
- D.**
SNMP traps

Answer: A

QUESTION NO: 67

The management team notices that new accounts that are set up manually do not always have correct access or permissions.

Which of the following automation techniques should a systems administrator use to streamline account creation?

- A.**
Guard rail script
- B.**
Ticketing workflow
- C.**
Escalation script
- D.**
User provisioning script

Answer: D

QUESTION NO: 68

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

- A.**
Corrective
- B.**
Preventive
- C.**
Detective
- D.**
Deterrent

Answer: C

QUESTION NO: 69

A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

- A.**
Serverless framework
- B.**
Type 1 hypervisor
- C.**
SD-WAN
- D.**
SDN

Answer: A

QUESTION NO: 70

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

- A.
Tuning
- B.
Aggregating
- C.
Quarantining
- D.
Archiving

Answer: A

QUESTION NO: 71

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the **best** explanation for what the security analyst has discovered?

- A.
The user jsmith's account has been locked out.
- B.
A keylogger is installed on jsmith's workstation.
- C.
An attacker is attempting to brute force jsmith's account.
- D.
Ransomware has been deployed in the domain.

Answer: C

QUESTION NO: 72

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

- A.**
Clustering servers
- B.**
Geographic dispersion
- C.**
Load balancers
- D.**
Off-site backups

Answer: B

QUESTION NO: 73

Which of the following is a **primary** security concern for a company setting up a BYOD program?

- A.**
End of life
- B.**
Buffer overflow
- C.**
VM escape
- D.**
Jailbreaking

Answer: D

QUESTION NO: 74

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.

Which of the following analysis elements did the company **most** likely use in making this decision?

- A.
MTTR
- B.
RTO
- C.
ARO
- D.
MTBF

Answer: C

QUESTION NO: 75

Which of the following is the **most** likely to be included as an element of communication in a security awareness program?

- A.
Reporting phishing attempts or other suspicious activities
- B.
Detecting insider threats using anomalous behavior recognition
- C.
Verifying information when modifying wire transfer data
- D.
Performing social engineering as part of third-party penetration testing

Answer: A

QUESTION NO: 76 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.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- 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	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- 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	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- 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	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- 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	- Botnet - RAT - Logic Bomb - Backdoor - Virus - Spyware - Worm - Adware - Ransomware - Keylogger - Phishing	- 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

Explanation:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	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	Virus	Patch vulnerable systems
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

QUESTION NO: 77 HOTSPOT

You are a security administrator investigating a potential infection on a network.

INSTRUCTIONS

Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.

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

192.168.10.22

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31 Warn Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32 Warn Scheduled update disabled by process scvh0st.exe
```

192.168.10.37

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

192.168.10.41

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

Firewall



Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

10.10.9.12



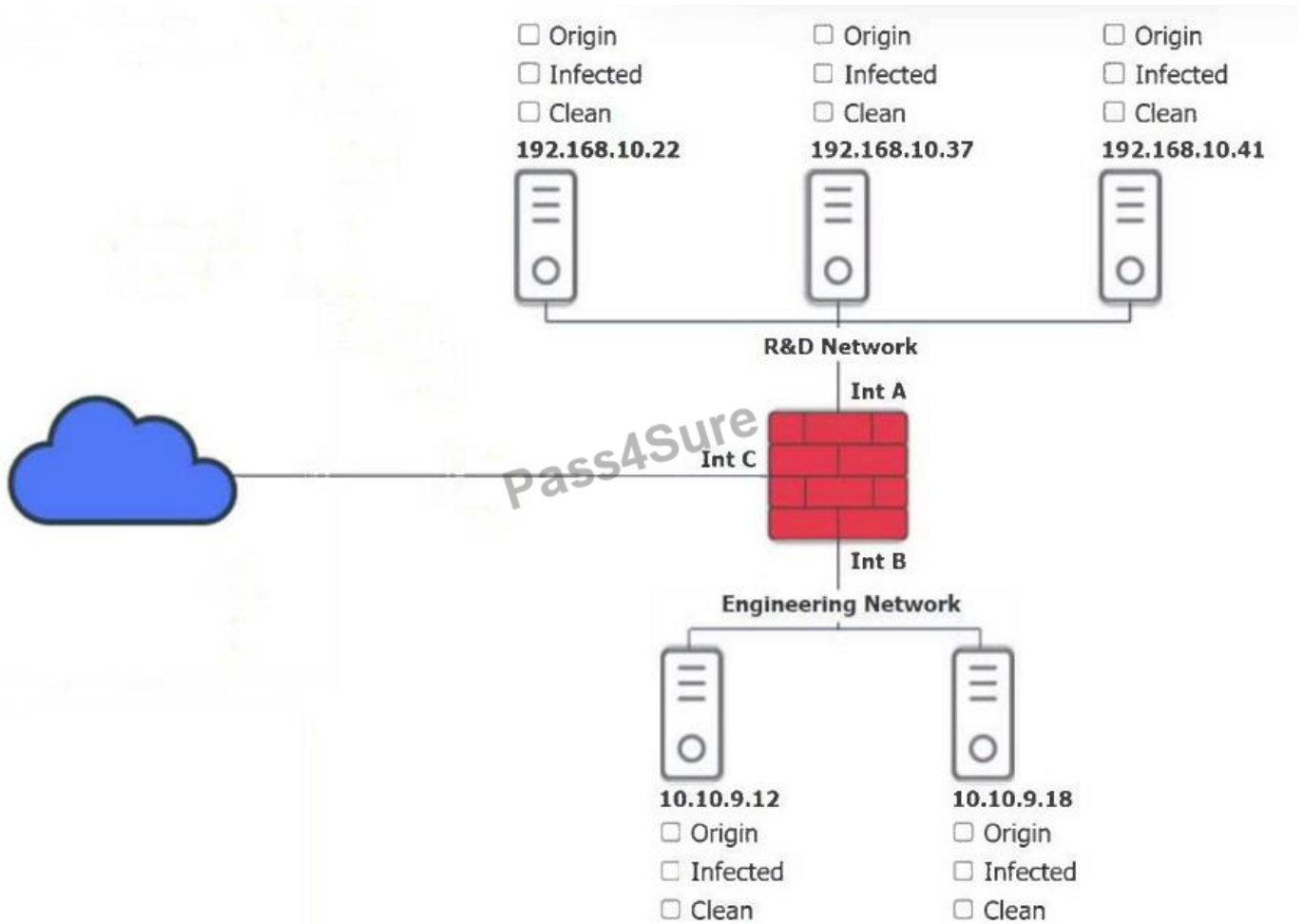
```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

10.10.9.18

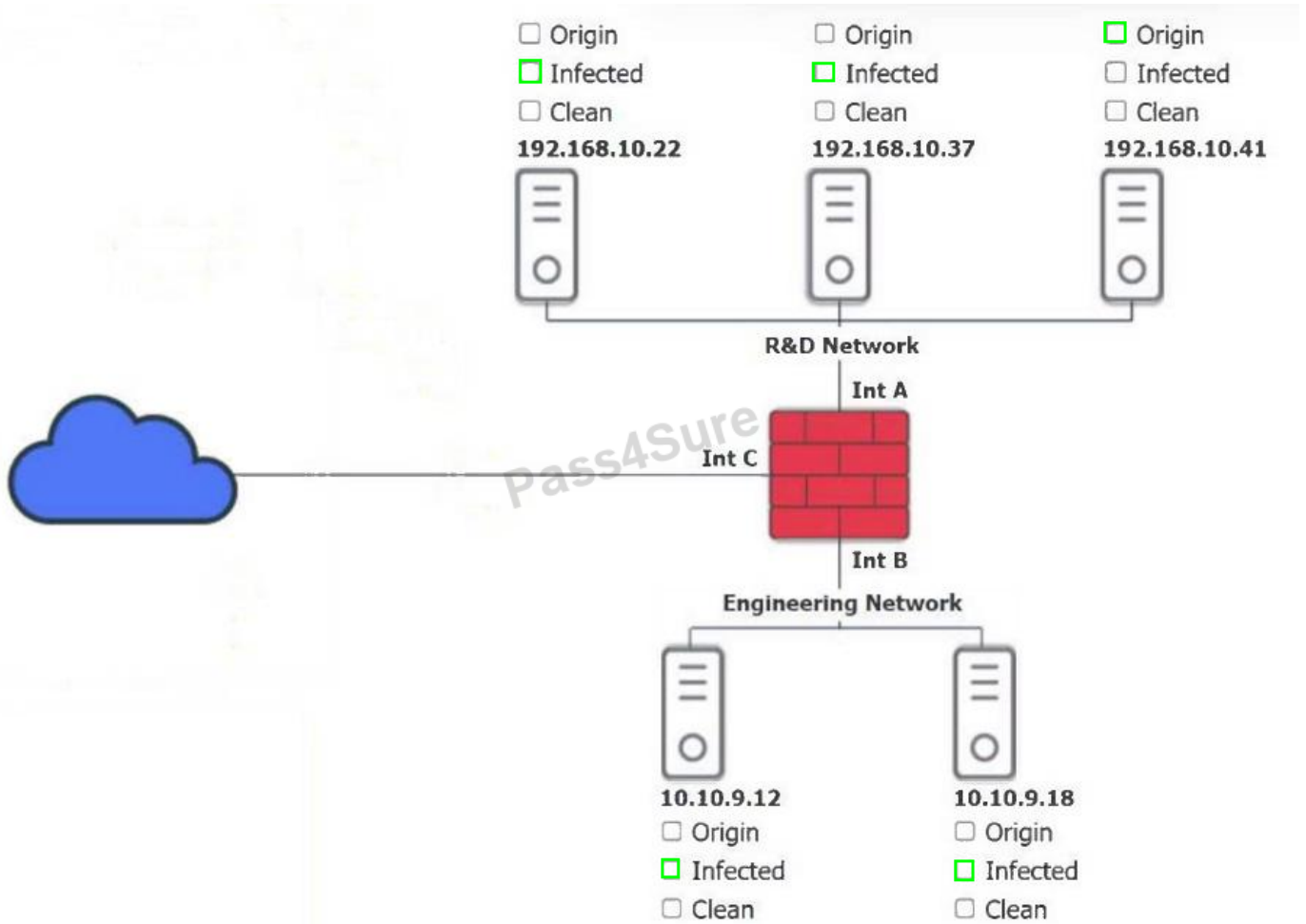
```

4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

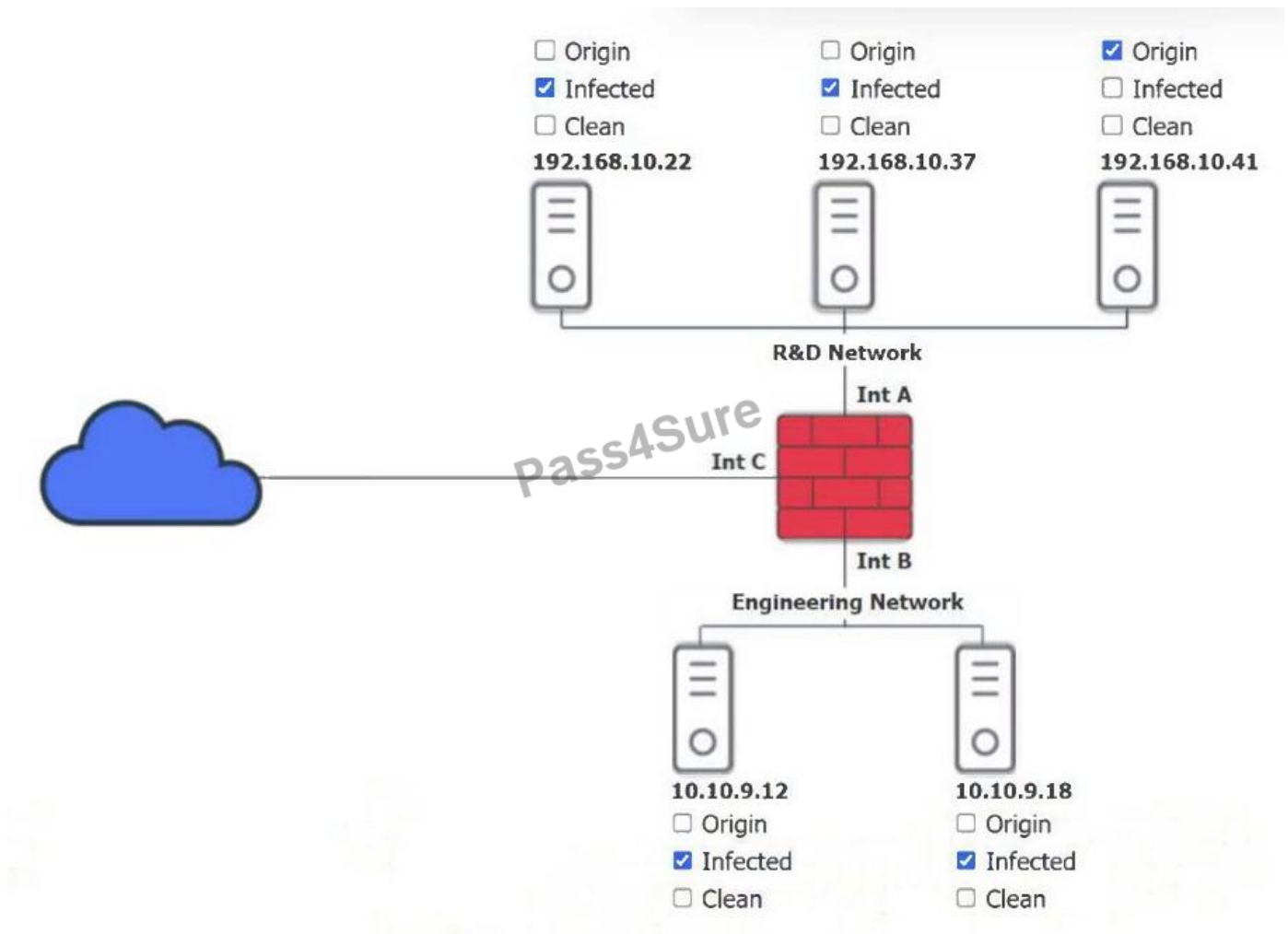
```



Answer:



Explanation:

**QUESTION NO: 78**

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

- A.**
Preparation
- B.**
Recovery
- C.**
Lessons learned
- D.**
Analysis

Answer: A

QUESTION NO: 79

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A.**
Console access
- B.**
Routing protocols
- C.**
VLANs
- D.**
Web-based administration

Answer: D

QUESTION NO: 80

A security administrator needs a method to secure data in an environment that includes some form of checks so track any changes. Which of the following should the administrator set up to achieve this goal?

- A.**
SPF
- B.**
GPO
- C.**
NAC
- D.**
FIM

Answer: D

QUESTION NO: 81

An administrator is reviewing a single server's security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	09/16/2022 11:13:05 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:07 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:09 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:11 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:13 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:15 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:17 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:19 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:21 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:23 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:25 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:27 AM	Microsoft Windows security	4625	Logon

Which of the following best describes the action captured in this log file?

- A.
Brute-force attack
- B.
Privilege escalation
- C.
Failed password audit
- D.
Forgotten password by the user

Answer: A

QUESTION NO: 82

A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Choose two.)

- A.**
Key escrow
- B.**
TPM presence
- C.**
Digital signatures
- D.**
Data tokenization
- E.**
Public key management
- F.**
Certificate authority linking

Answer: A,B

QUESTION NO: 83

A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

- A.**
Changing the remote desktop port to a non-standard number
- B.**
Setting up a VPN and placing the jump server inside the firewall
- C.**
Using a proxy for web connections from the remote desktop server
- D.**
Connecting the remote server to the domain and increasing the password length

Answer: B

QUESTION NO: 84

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A.**
ACL
- B.**
DLP
- C.**
IDS
- D.**
IPS

Answer: C

QUESTION NO: 85

Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

- A.**
Remote access points should fail closed.
- B.**
Logging controls should fail open.
- C.**
Safety controls should fail open.
- D.**
Logical security controls should fail closed.

Answer: C

QUESTION NO: 86

Which of the following would be best suited for constantly changing environments?

- A.**
RTOS
- B.**
Containers
- C.**
Embedded systems
- D.**
SCADA

Answer: B

QUESTION NO: 87

Which of the following incident response activities ensures evidence is properly handled?

- A.**
E-discovery
- B.**
Chain of custody
- C.**
Legal hold
- D.**
Preservation

Answer: A

QUESTION NO: 88

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account. Which of the following would most likely prevent this activity in the future?

- A.**
Standardizing security incident reporting

- B.**
Executing regular phishing campaigns
- C.**
Implementing insider threat detection measures
- D.**
Updating processes for sending wire transfers

Answer: D

QUESTION NO: 89

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

- A.**
Off-the-shelf software
- B.**
Orchestration
- C.**
Baseline
- D.**
Policy enforcement

Answer: B

QUESTION NO: 90

A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

- A.**
Processor
- B.**
Custodian

C.
Subject

D.
Owner

Answer: C

QUESTION NO: 91

Which of the following describes the maximum allowance of accepted risk?

A.
Risk indicator

B.
Risk level

C.
Risk score

D.
Risk threshold

Answer: D

QUESTION NO: 92

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A.
A worm is propagating across the network.

B.
Data is being exfiltrated.

C.
A logic bomb is deleting data.

D.
Ransomware is encrypting files.

Answer: B

QUESTION NO: 93

A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

- A.**
Default credentials
- B.**
Non-segmented network
- C.**
Supply chain vendor
- D.**
Vulnerable software

Answer: C

QUESTION NO: 94

A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

- A.**
Zero Trust
- B.**
AAA
- C.**
Non-repudiation
- D.**

CIA

Answer: A

QUESTION NO: 95

Which of the following involves an attempt to take advantage of database misconfigurations?

- A.**
Buffer overflow
- B.**
SQL injection
- C.**
VM escape
- D.**
Memory injection

Answer: B

QUESTION NO: 96

Which of the following is used to validate a certificate when it is presented to a user?

- A.**
OCSP
- B.**
CSR
- C.**
CA
- D.**
CRC

Answer: A

QUESTION NO: 97

One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

- A.**
Virtualization
- B.**
Firmware
- C.**
Application
- D.**
Operating system

Answer: B

QUESTION NO: 98

Which of the following is used to quantitatively measure the criticality of a vulnerability?

- A.**
CVE
- B.**
CVSS
- C.**
CIA
- D.**
CERT

Answer: B

QUESTION NO: 99

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- A.**
Configure all systems to log scheduled tasks.

B.

Collect and monitor all traffic exiting the network.

C.

Block traffic based on known malicious signatures.

D.

Install endpoint management software on all systems

Answer: D

QUESTION NO: 100

An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

A.

Data in use

B.

Data in transit

C.

Geographic restrictions

D.

Data sovereignty

Answer: B

QUESTION NO: 101

After reviewing the following vulnerability scanning report:

```
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
```

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption

PORT      STATE SERVICE REASON
23/tcp    open  telnet  syn-ack
| telnet encryption:
|_ Telnet server supports encryption
```

Which of the following would the security analyst conclude for this reported vulnerability?

- A.**
It is a false positive.
- B.**
A rescan is required.
- C.**
It is considered noise.
- D.**
Compensating controls exist.

Answer: D

QUESTION NO: 102

An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system. Which of the following best describes the actions taken by the organization?

- A.**
Exception
- B.**
Segmentation
- C.**
Risk transfer
- D.**
Compensating controls

Answer: B

QUESTION NO: 103

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

- A.**
EAP
- B.**
DHCP
- C.**
IPSec
- D.**
NAT

Answer: C

QUESTION NO: 104

Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

- A.**
Software as a service
- B.**
Infrastructure as code
- C.**
Internet of Things
- D.**
Software-defined networking

Answer: B

QUESTION NO: 105

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

- A.**
Insider threat
- B.**
Email phishing
- C.**
Social engineering
- D.**
Executive whaling

Answer: C

QUESTION NO: 106

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

- A.**
Block access to cloud storage websites.
- B.**
Create a rule to block outgoing email attachments.
- C.**
Apply classifications to the data.
- D.**
Remove all user permissions from shares on the file server.

Answer: C

QUESTION NO: 107

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

- A.
Compromise
- B.
Retention
- C.
Analysis
- D.
Transfer
- E.
Inventory

Answer: B

QUESTION NO: 108

A company is working with a vendor to perform a penetration test. Which of the following includes an estimate about the number of hours required to complete the engagement?

- A.
SOW
- B.
BPA
- C.
SLA
- D.
NDA

Answer: A

QUESTION NO: 109

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following **best** describes the threat actor in the CISO's report?

- A.

Insider threat

B.

Hacktivist

C.

Nation-state

D.

Organized crime

Answer: D

QUESTION NO: 110

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

A.

Code scanning for vulnerabilities

B.

Open-source component usage

C.

Quality assurance testing

D.

Peer review and approval

Answer: D

QUESTION NO: 111

Which of the following can best protect against an employee inadvertently installing malware on a company system?

A.

Host-based firewall

B.

System isolation

C.

Least privilege

D.

Application allow list

Answer: D

QUESTION NO: 112

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A.

Cross-site scripting

B.

Buffer overflow

C.

Jailbreaking

D.

Side loading

Answer: C

QUESTION NO: 113

Which of the following would be the **best** ways to ensure only authorized personnel can access a secure facility? (Choose two.)

A.

Fencing

B.

Video surveillance

C.

Badge access

D.

Access control vestibule

E.

Sign-in sheet

F.

Sensor

Answer: C,D

QUESTION NO: 114

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A.

Segmentation

B.

Isolation

C.

Patching

D.

Encryption

Answer: A

QUESTION NO: 115

Which of the following is the most common data loss path for an air-gapped network?

A.

Bastion host

B.

Unsecured Bluetooth

C.

Unpatched OS

D.
Removable devices

Answer: D

QUESTION NO: 116

Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A.
Impersonation

B.
Disinformation

C.
Watering-hole

D.
Smishing

Answer: C

QUESTION NO: 117

An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

A.
Deploying a SASE solution to remote employees

B.
Building a load-balanced VPN solution with redundant internet

C.
Purchasing a low-cost SD-WAN solution for VPN traffic

D.
Using a cloud provider to create additional VPN concentrators

Answer: A

QUESTION NO: 118

Which of the following is the **best** reason to complete an audit in a banking environment?

- A.**
Regulatory requirement
- B.**
Organizational change
- C.**
Self-assessment requirement
- D.**
Service-level requirement

Answer: A

QUESTION NO: 119

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

- A.**
Integrity
- B.**
Availability
- C.**
Confidentiality
- D.**
Non-repudiation

Answer: C

QUESTION NO: 120

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Choose two.)

A.

The device has been moved from a production environment to a test environment.

B.

The device is configured to use cleartext passwords.

C.

The device is moved to an isolated segment on the enterprise network.

D.

The device is moved to a different location in the enterprise.

E.

The device's encryption level cannot meet organizational standards.

F.

The device is unable to receive authorized updates.

Answer: E,F

QUESTION NO: 121

A company is required to perform a risk assessment on an annual basis. Which of the following types of risk assessments does this requirement describe?

A.

Continuous

B.

Ad hoc

C.

Recurring

D.

One time

Answer: C

QUESTION NO: 122

After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

- A.**
Compensating
- B.**
Detective
- C.**
Preventive
- D.**
Corrective

Answer: B

QUESTION NO: 123

Which of the following exercises should an organization use to improve its incident response process?

- A.**
Tabletop
- B.**
Replication
- C.**
Failover
- D.**
Recovery

Answer: A

QUESTION NO: 124

Which of the following best ensures minimal downtime and data loss for organizations with critical computing equipment located in earthquake-prone areas?

- A.**

Generators and UPS

B.

Off-site replication

C.

Redundant cold sites

D.

High availability networking

Answer: B

QUESTION NO: 125

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A.

Insurance

B.

Patching

C.

Segmentation

D.

Replacement

Answer: C

QUESTION NO: 126

After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

A.

Group Policy

B.

Content filtering

- C.**
Data loss prevention
- D.**
Access control lists

Answer: D

QUESTION NO: 127

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A.**
MOA
- B.**
SOW
- C.**
MOU
- D.**
SLA

Answer: D

QUESTION NO: 128

A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

- A.**
Certification
- B.**
Inventory list
- C.**
Classification
- D.**

Proof of ownership

Answer: A

QUESTION NO: 129

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

- A.**
Geographic dispersion
- B.**
Platform diversity
- C.**
Hot site
- D.**
Load balancing

Answer: A

QUESTION NO: 130

A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

- A.**
Obtain the file's SHA-256 hash.
- B.**
Use hexdump on the file's contents.
- C.**
Check endpoint logs.
- D.**
Query the file's metadata.

Answer: D

QUESTION NO: 131

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

- A.**
Red
- B.**
Blue
- C.**
Purple
- D.**
Yellow

Answer: C

QUESTION NO: 132

A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

- A.**
Patch availability
- B.**
Product software compatibility
- C.**
Ease of recovery
- D.**
Cost of replacement

Answer: A

QUESTION NO: 133

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

- A.**
A full inventory of all hardware and software
- B.**
Documentation of system classifications
- C.**
A list of system owners and their departments
- D.**
Third-party risk assessment documentation

Answer: A

QUESTION NO: 134

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A.**
Impact analysis
- B.**
Scheduled downtime
- C.**
Backout plan
- D.**
Change management boards

Answer: B

QUESTION NO: 135

A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

- A.**
Hashing
- B.**
Tokenization
- C.**
Encryption
- D.**
Segmentation

Answer: C

QUESTION NO: 136

A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?

- A.**
End of business
- B.**
End of testing
- C.**
End of support
- D.**
End of life

Answer: D

QUESTION NO: 137

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

- A.**
Encryption at rest
- B.**
Masking

- C.**
Data classification
- D.**
Permission restrictions

Answer: A

QUESTION NO: 138

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

- A.**
Concurrent session usage
- B.**
Secure DNS cryptographic downgrade
- C.**
On-path resource consumption
- D.**
Reflected denial of service

Answer: D

QUESTION NO: 139

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

- A.**
RBAC
- B.**
ACL

- C.
SAML
- D.
GPO

Answer: A

QUESTION NO: 140

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Choose two.)

- A.
Federation
- B.
Identity proofing
- C.
Password complexity
- D.
Default password changes
- E.
Password manager
- F.
Open authentication

Answer: A,C

QUESTION NO: 141

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

- A.

SIEM

B.

DLP

C.

IDS

D.

SNMP

Answer: A

QUESTION NO: 142

A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

Something you know

Something you have

Something you are

Which of the following would accomplish the manager's goal?

A.

Domain name, PKI, GeoIP lookup

B.

VPN IP address, company ID, facial structure

C.

Password, authentication token, thumbprint

D.

Company URL, TLS certificate, home address

Answer: C

QUESTION NO: 143

Which of the following would be the best way to handle a critical business application that is

running on a legacy server?

- A.**
Segmentation
- B.**
Isolation
- C.**
Hardening
- D.**
Decommissioning

Answer: A

QUESTION NO: 144

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

- A.**
VM escape
- B.**
SQL injection
- C.**
Buffer overflow
- D.**
Race condition

Answer: C

QUESTION NO: 145

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

- A.**

Retain the emails between the security team and affected customers for 30 days.

- B.**
Retain any communications related to the security breach until further notice.
- C.**
Retain any communications between security members during the breach response.
- D.**
Retain all emails from the company to affected customers for an indefinite period of time.

Answer: B

QUESTION NO: 146

Which of the following describes the process of concealing code or text inside a graphical image?

- A.**
Symmetric encryption
- B.**
Hashing
- C.**
Data masking
- D.**
Steganography

Answer: D

QUESTION NO: 147

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

- A.**
Vishing
- B.**
Smishing

C.
Pretexting

D.
Phishing

Answer: B

QUESTION NO: 148

Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

A.
Mitigate

B.
Accept

C.
Transfer

D.
Avoid

Answer: A

QUESTION NO: 149

Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule. Which of the following best describes this form of security control?

A.
Physical

B.
Managerial

C.
Technical

D.

Operational

Answer: A

QUESTION NO: 150

The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening?

- A.**
Using least privilege
- B.**
Changing the default password
- C.**
Assigning individual user IDs
- D.**
Reviewing logs more frequently

Answer: B

QUESTION NO: 151

Which of the following is the best way to secure an on-site data center against intrusion from an insider?

- A.**
Bollards
- B.**
Access badge
- C.**
Motion sensor
- D.**
Video surveillance

Answer: B

QUESTION NO: 152

An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?

- A.**
Role-based
- B.**
Discretionary
- C.**
Time of day
- D.**
Least privilege

Answer: A

QUESTION NO: 153

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Choose two.)

- A.**
Channels by which the organization communicates with customers
- B.**
The reporting mechanisms for ethics violations
- C.**
Threat vectors based on the industry in which the organization operates
- D.**
Secure software development training for all personnel
- E.**
Cadence and duration of training events
- F.**
Retraining requirements for individuals who fail phishing simulations

Answer: B,F

QUESTION NO: 154

A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfil?

- A.**
Privacy
- B.**
Integrity
- C.**
Confidentiality
- D.**
Availability

Answer: D

QUESTION NO: 155

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

- A.**
Deploying PowerShell scripts
- B.**
Pushing GPO update
- C.**
Enabling PAP
- D.**
Updating EDR profiles

Answer: B

QUESTION NO: 156

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

- A.**
ARO
- B.**
RTO
- C.**
RPO
- D.**
ALE
- E.**
SLE

Answer: D

QUESTION NO: 157

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

- A.**
Key stretching
- B.**
Tokenization
- C.**
Data masking
- D.**
Salting

Answer: D

QUESTION NO: 158

A technician is deploying a new security camera. Which of the following should the technician do?

- A.**
Configure the correct VLAN.
- B.**
Perform a vulnerability scan.
- C.**
Disable unnecessary ports.
- D.**
Conduct a site survey.

Answer: C

QUESTION NO: 159

A company is experiencing a web services outage on the public network. The services are up and available but inaccessible. The network logs show a sudden increase in network traffic that is causing the outage. Which of the following attacks is the organization experiencing?

- A.**
ARP poisoning
- B.**
Brute force
- C.**
Buffer overflow
- D.**
DDoS

Answer: D

QUESTION NO: 160

Which of the following threat actors is the most likely to be motivated by profit?

- A.**
Hacktivist

- B.**
Insider threat
- C.**
Organized crime
- D.**
Shadow IT

Answer: C

QUESTION NO: 161

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Choose two.)

- A.**
Application
- B.**
Authentication
- C.**
DHCP
- D.**
Network
- E.**
Firewall
- F.**
Database

Answer: C,E

QUESTION NO: 162

During a penetration test, a vendor attempts to enter an unauthorized area using an access badge. Which of the following types of tests does this represent?

- A.**
Defensive

- B.**
Passive
- C.**
Offensive
- D.**
Physical

Answer: D

QUESTION NO: 163

A systems administrator uses a key to encrypt a message being sent to a peer in a different branch office. The peer then uses the same key to decrypt the message. Which of the following describes this example?

- A.**
Symmetric
- B.**
Asymmetric
- C.**
Hashing
- D.**
Salting

Answer: A

QUESTION NO: 164

A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?

- A.**
Port security
- B.**
Web application firewall

- C.**
Transport layer security
- D.**
Virtual private network

Answer: A

QUESTION NO: 165

A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Choose two.)

- A.**
Data retention
- B.**
Certification
- C.**
Destruction
- D.**
Classification
- E.**
Sanitization
- F.**
Enumeration

Answer: C,E

QUESTION NO: 166

A systems administrator would like to deploy a change to a production system. Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

- A.**
Backout plan
- B.**

Impact analysis

C.

Test procedure

D.

Approval procedure

Answer: A

QUESTION NO: 167

A company is redesigning its infrastructure and wants to reduce the number of physical servers in use. Which of the following architectures is best suited for this goal?

A.

Serverless

B.

Segmentation

C.

Virtualization

D.

Microservices

Answer: C

QUESTION NO: 168

A bank set up a new server that contains customers' PII. Which of the following should the bank use to make sure the sensitive data is not modified?

A.

Full disk encryption

B.

Network access control

C.

File integrity monitoring

D.
User behavior analytics

Answer: C

QUESTION NO: 169

Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked. Which of the following changes would allow users to access the site?

- A.**
Creating a firewall rule to allow HTTPS traffic
- B.**
Configuring the IPS to allow shopping
- C.**
Tuning the DLP rule that detects credit card data
- D.**
Updating the categorization in the content filter

Answer: D

QUESTION NO: 170

Which of the following **most** impacts an administrator's ability to address CVEs discovered on a server?

- A.**
Rescanning requirements
- B.**
Patch availability
- C.**
Organizational impact
- D.**
Risk tolerance

Answer: B

QUESTION NO: 171

Which of the following describes effective change management procedures?

- A.**
Approving the change after a successful deployment
- B.**
Having a backout plan when a patch fails
- C.**
Using a spreadsheet for tracking changes
- D.**
Using an automatic change control bypass for security updates

Answer: B

QUESTION NO: 172

The CIRT is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?

- A.**
WAF utilizing SSL decryption
- B.**
NGFW utilizing application inspection
- C.**
UTM utilizing a threat feed
- D.**
SD-WAN utilizing IPSec

Answer: B

QUESTION NO: 173

An enterprise is working with a third party and needs to allow access between the internal networks of both parties for a secure file migration. The solution needs to ensure encryption is applied to all traffic that is traversing the networks. Which of the following solutions should **most** likely be implemented?

- A.**
EAP
- B.**
IPSec
- C.**
SD-WAN
- D.**
TLS

Answer: B

QUESTION NO: 174

An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following **best** describes the tool the administrator is using?

- A.**
DLP
- B.**
SNMP traps
- C.**
SCAP
- D.**
IPS

Answer: A

QUESTION NO: 175

A software developer released a new application and is distributing application files via the developer's website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

- A.
Hashes
- B.
Certificates
- C.
Algorithms
- D.
Salting

Answer: A

QUESTION NO: 176

An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team **most** likely to recommend?

- A.
Tokenization
- B.
Hashing
- C.
Obfuscation
- D.
Segmentation

Answer: B

QUESTION NO: 177

An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

- A.
Virus
- B.
Trojan
- C.
Spyware
- D.
Ransomware

Answer: D

QUESTION NO: 178

A systems administrator is advised that an external web server is not functioning properly. The administrator reviews the following firewall logs containing traffic going to the web server:

Date	Time	SourceIP	SPort	Flag	DestIP	DPort
2023-01-25	01:45:09.102	98.123.45.100	4560	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	95.123.45.101	3361	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	99.123.45.102	3662	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	89.123.45.103	5663	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	98.123.45.104	4064	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	80.123.45.105	4365	SYN	100.50.20.7	443

Which of the following attacks is likely occurring?

- A.
DDoS
- B.
Directory traversal
- C.
Brute-force
- D.
HTTPS downgrade

Answer: A

QUESTION NO: 179

An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?

- A.**
Recovery point objective
- B.**
Mean time between failures
- C.**
Recovery time objective
- D.**
Mean time to repair

Answer: D

QUESTION NO: 180

A security engineer is installing an IPS to block signature-based attacks in the environment.

Which of the following modes will best accomplish this task?

- A.**
Monitor
- B.**
Sensor
- C.**
Audit
- D.**
Active

Answer: D

Reference: <https://www.geeksforgeeks.org/intrusion-prevention-system-ips/>

QUESTION NO: 181

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

- A.**
XDR
- B.**
SPF
- C.**
DLP
- D.**
DMARC

Answer: C

Reference: <https://gttb.com/2022/07/06/xdr-extended-detection-and-response-vs-dlp/>

QUESTION NO: 182

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- A.**
IDS
- B.**
ACL
- C.**
EDR
- D.**
NAC

Answer: C

Reference: <https://www.malwarebytes.com/solutions>

QUESTION NO: 183

Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following **best** describes this security concept?

- A.**
Availability
- B.**
Confidentiality
- C.**
Integrity
- D.**
Non-repudiation

Answer: B

QUESTION NO: 184

Which of the following describes the category of data that is **most** impacted when it is lost?

- A.**
Confidential
- B.**
Public
- C.**
Private
- D.**
Critical

Answer: D

Reference: <https://corporatefinanceinstitute.com/resources/data-science/data-loss/>

QUESTION NO: 185

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is **most** likely being used?

- A.**
Business email
- B.**
Social engineering
- C.**
Unsecured network
- D.**
Default credentials

Answer: B

QUESTION NO: 186

Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

- A.**
SLA
- B.**
MOU
- C.**
MOA
- D.**
BPA

Answer: A

Reference: <https://blog.logrocket.com/product-management/service-level-agreement-sla-definition-templates-examples/>

QUESTION NO: 187

A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations. Which of the following is the **best** type of site for this company?

- A.**
Cold
- B.**
Tertiary
- C.**
Warm
- D.**
Hot

Answer: D

Reference: <https://www.nakivo.com/blog/overview-disaster-recovery-sites/>

QUESTION NO: 188

Which of the following security controls is **most** likely being used when a critical legacy server is segmented into a private network?

- A.**
Deterrent
- B.**
Corrective
- C.**
Compensating
- D.**
Preventive

Answer: C

Reference: <https://www.infosecurity-magazine.com/blogs/protecting-legacy-systems-modern-1/>

QUESTION NO: 189

Which of the following **best** describes the practice of researching laws and regulations related to information security operations within a specific industry?

- A.**
Compliance reporting
- B.**
GDPR
- C.**
Due diligence
- D.**
Attestation

Answer: C

QUESTION NO: 190

Which of the following considerations is the **most** important for an organization to evaluate as it establishes and maintains a data privacy program?

- A.**
Reporting structure for the data privacy officer
- B.**
Request process for data subject access
- C.**
Role as controller or processor
- D.**
Physical location of the company

Answer: C

Reference: <https://www.pivotpointsecurity.com/10-most-important-steps-to-build-a-data-privacy-program/>

QUESTION NO: 191

A security analyst is investigating a workstation that is suspected of outbound communication to a command-and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted. Which of the following logs would the analyst most likely look at **next**?

- A.**
IPS
- B.**
Firewall
- C.**
ACL
- D.**
Windows security

Answer: B

QUESTION NO: 192

An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?

- A.**
Business continuity
- B.**
Physical security
- C.**
Change management
- D.**
Disaster recovery

Answer: A

Reference: <https://creately.com/guides/incident-management/>

QUESTION NO: 193

A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the **best** option?

- A.**
Hot
- B.**
Cold
- C.**
Warm
- D.**
Geographically dispersed

Answer: C

Reference: <https://www.nakivo.com/blog/overview-disaster-recovery-sites/>

QUESTION NO: 194

A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

- A.**
Virtualization and isolation of resources
- B.**
Network segmentation
- C.**
Data encryption
- D.**
Strong authentication policies

Answer: A

Reference: <https://www.microsoft.com/en-us/security/blog/2023/07/05/11-best-practices-for-securing-data-in-cloud-services/>

QUESTION NO: 195

A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?

- A.**
End user training
- B.**
Policy review
- C.**
URL scanning
- D.**
Plain text email

Answer: A

QUESTION NO: 196

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the **best** way for the company to confirm this information?

- A.**
Validate the code signature.
- B.**
Execute the code in a sandbox.
- C.**
Search the executable for ASCII strings.
- D.**
Generate a hash of the files.

Answer: A

Reference: <https://seon.io/resources/comparisons/identity-verification-software-tools/>

QUESTION NO: 197

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?

- A.**
Installing HIDS on the system
- B.**
Placing the system in an isolated VLAN
- C.**
Decommissioning the system
- D.**
Encrypting the system's hard drive

Answer: B

Reference: https://resources.trendmicro.com/rs/945-CXD-062/images/WP01_Protecting_EOS_Systems_190719US_web.pdf

QUESTION NO: 198

The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators. Which of the following should the CISO use?

- A.**
Penetration test
- B.**
Internal audit
- C.**
Attestation
- D.**
External examination

Answer: B

Reference: <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules/ciso-role-in-cyber-disclosure.html>

QUESTION NO: 199

A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?

- A.**
Espionage
- B.**
Data exfiltration
- C.**
Nation-state attack
- D.**
Shadow IT

Answer: D

QUESTION NO: 200

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

- A.**
Shadow IT
- B.**
Insider threat
- C.**
Data exfiltration
- D.**
Service disruption

Answer: A

Reference: <https://www.fortinet.com/resources/cyberglossary/shadow-it>

QUESTION NO: 201

Which of the following would **best** explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

- A.**
To track the status of patching installations
- B.**
To find shadow IT cloud deployments
- C.**
To continuously the monitor hardware inventory
- D.**
To hunt for active attackers in the network

Answer: A

Reference: <https://www.syxsense.com/why-vulnerability-security-scanning-is-crucial-for-endpoint-management>

QUESTION NO: 202

Which of the following is classified as high availability in a cloud environment?

- A.**
Access broker
- B.**
Cloud HSM
- C.**
WAF
- D.**
Load balancer

Answer: D

Reference: <https://www.economize.cloud/glossary/high-availability>

QUESTION NO: 203

Which of the following security measures is required when using a cloud-based platform for IoT management?

- A.**
Encrypted connection
- B.**
Federated identity
- C.**
Firewall
- D.**
Single sign-on

Answer: A

Reference: <https://learn.microsoft.com/en-us/azure/iot/iot-overview-security>

QUESTION NO: 204

Which of the following threat vectors is **most** commonly utilized by insider threat actors attempting data exfiltration?

- A.**
Unidentified removable devices
- B.**
Default network device credentials
- C.**
Spear phishing emails
- D.**
Impersonation of business units through typosquatting

Answer: A

Reference: <https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/06/09/insider-data-exfiltration---threats-and-new-challenges>

QUESTION NO: 205

Which of the following methods to secure credit card data is **best** to use when a requirement is to see only the last four numbers on a credit card?

- A.**
Encryption
- B.**
Hashing
- C.**
Masking
- D.**
Tokenization

Answer: C

Reference: <https://money.stackexchange.com/questions/98951/credit-card-number-masking-good-practices-rules-law-regulations>

QUESTION NO: 206

The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?

- A.**
Fines
- B.**
Reputational damage
- C.**

Sanctions

D.

Contractual implications

Answer: A

Reference: <https://education.securiti.ai/certifications/privacyops/privacy/data-protection-consequences/>

QUESTION NO: 207

Which of the following alert types is the **most** likely to be ignored over time?

A.

True positive

B.

True negative

C.

False positive

D.

False negative

Answer: C

Reference: <https://fieldeffect.com/blog/cyber-security-alert-fatigue>

QUESTION NO: 208

A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

A.

Memory injection

- B.**
Race condition
- C.**
Side loading
- D.**
SQL injection

Answer: A

Reference: <https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/>

QUESTION NO: 209

An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

- A.**
Asset inventory
- B.**
Network enumeration
- C.**
Data certification
- D.**
Procurement process

Answer: A

Reference: <https://www.motadata.com/blog/patch-management/>

QUESTION NO: 210

Which of the following should a security operations center use to improve its incident response procedure?

- A.**
Playbooks
- B.**
Frameworks
- C.**
Baselines
- D.**
Benchmarks

Answer: A

Reference: <https://radiantsecurity.ai/learn/soc-incident-response/>

QUESTION NO: 211

Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?

- A.**
Continuity of operations
- B.**
Capacity planning
- C.**
Tabletop exercise
- D.**
Parallel processing

Answer: C

Reference: <https://www.businesstechweekly.com/cybersecurity/network-security/incident-response-plan-testing/>

QUESTION NO: 212

A healthcare organization wants to provide a web application that allows individuals to digitally

report health emergencies. Which of the following is the **most** important consideration during development?

- A.**
Scalability
- B.**
Availability
- C.**
Cost
- D.**
Ease of deployment

Answer: B

Reference: https://healthcareready.org/wp-content/uploads/2019/12/HCR_Telehealth_Brief_SCREEN_2.pdf

QUESTION NO: 213

Which of the following agreement types defines the time frame in which a vendor needs to respond?

- A.**
SOW
- B.**
SLA
- C.**
MOA
- D.**
MOU

Answer: B

Reference: <https://aws.amazon.com/what-is/service-level-agreement/>

QUESTION NO: 214

Which of the following is a feature of a next-generation SIEM system?

- A.**
Virus signatures
- B.**
Automated response actions
- C.**
Security agent deployment
- D.**
Vulnerability scanning

Answer: B

Reference: <https://panther.com/cyber-explained/next-gen-siem/>

QUESTION NO: 215

To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following **best** describe these types of controls? (Choose two.)

- A.**
Preventive
- B.**
Deterrent
- C.**
Corrective
- D.**
Directive
- E.**
Compensating
- F.**
Detective

Answer: B,F

Reference: <https://hiksec.com/secure-spaces-with-cctv-and-access-control-systems/>

QUESTION NO: 216

Which of the following examples would be **best** mitigated by input sanitization?

A.

`<script>alert("Warning!");</script>`

B.

`nmap - 10.11.1.130`

C.

Email message: "Click this link to get your free gift card."

D.

Browser message: "Your connection is not private."

Answer: A

Reference: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

QUESTION NO: 217

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A.

Smishing

B.

Disinformation

C.

Impersonating

D.

Whaling

Answer: C

Reference: <https://digitalsecurityguide.eset.com/en-us/impersonation-when-an-attacker-is-posing-as-the-ceo>

QUESTION NO: 218

After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned. Which of the following describes this example?

- A.**
False positive
- B.**
False negative
- C.**
True positive
- D.**
True negative

Answer: A

Reference: <https://www.itgovernance.co.uk/blog/vulnerability-scans-false-positives-the-importance-of-sanitising-input>

QUESTION NO: 219

A recent penetration test identified that an attacker could flood the MAC address table of network switches. Which of the following would **best** mitigate this type of attack?

- A.**
Load balancer
- B.**
Port security
- C.**
IPS

D.
NGFW

Answer: B

Reference: <https://www.interserver.net/tips/kb/mac-flooding-prevent/>

QUESTION NO: 220

A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?

- A.**
SQLi
- B.**
Cross-site scripting
- C.**
Jailbreaking
- D.**
Side loading

Answer: C

Reference: <https://www.wikihow.com/Allow-Apps-from-Unknown-Sources-on-Android>

QUESTION NO: 221

Which of the following phases of an incident response involves generating reports?

- A.**
Recovery
- B.**
Preparation
- C.**

Lessons learned

D.

Containment

Answer: C

Reference: <https://subrosacyber.com/en/blog/what-are-the-phases-of-incident-response>

QUESTION NO: 222

Which of the following methods would **most** likely be used to identify legacy systems?

A.

Bug bounty program

B.

Vulnerability scan

C.

Package monitoring

D.

Dynamic analysis

Answer: B

Reference: <https://www.stackscale.com/blog/legacy-systems/>

QUESTION NO: 223

Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following **best** describes this solution?

A.

Proxy server

B.

NGFW

C.
VPN

D.
Security zone

Answer: C

Reference: <https://www.beyondidentity.com/resource/secure-remote-access-what-is-it-and-best-practices>

QUESTION NO: 224

A company allows customers to upload PDF documents to its public e-commerce website. Which of the following would a security analyst **most** likely recommend?

A.
Utilizing attack signatures in an IDS

B.
Enabling malware detection through a UTM

C.
Limiting the affected servers with a load balancer

D.
Blocking command injections via a WAF

Answer: B

Reference: <https://blog.filestack.com/secure-file-upload/>

QUESTION NO: 225

A security analyst developed a script to automate a trivial and repeatable task. Which of the following **best** describes the benefits of ensuring other team members understand how the script works?

A.
To reduce implementation cost

B.

To identify complexity

C.

To remediate technical debt

D.

To prevent a single point of failure

Answer: D

Reference: <https://www.lambdatest.com/blog/automation-scripts/>

QUESTION NO: 226

A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?

A.

Microservices

B.

Containerization

C.

Virtualization

D.

Infrastructure as code

Answer: B

Reference: <https://phoenixnap.com/blog/server-consolidation>

QUESTION NO: 227

An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Choose two.)

- A.**
Disable default accounts.
- B.**
Add the server to the asset inventory.
- C.**
Remove unnecessary services.
- D.**
Document default passwords.
- E.**
Send server logs to the SIEM.
- F.**
Join the server to the corporate domain.

Answer: A,C

Reference: <https://www.ninjaone.com/blog/steps-of-a-server-hardening-process/>

QUESTION NO: 228

A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following will be the **best** method to achieve this objective?

- A.**
Third-party attestation
- B.**
Penetration testing
- C.**
Internal auditing
- D.**
Vulnerability scans

Answer: C

Reference: <https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/04/26/key-metrics-for-a-ciso-dashboard>

QUESTION NO: 229

Which of the following security concepts is accomplished with the installation of a RADIUS server?

- A.**
CIA
- B.**
AAA
- C.**
ACL
- D.**
PEM

Answer: B

Reference: <https://www.fortinet.com/resources/cyberglossary/radius-protocol>

QUESTION NO: 230

After creating a contract for IT contractors, the human resources department changed several clauses. The contract has gone through three revisions. Which of the following processes should the human resources department follow to track revisions?

- A.**
Version validation
- B.**
Version changes
- C.**
Version updates
- D.**
Version control

Answer: D

Reference: <https://www.contractlogix.com/contract-management/how-to-track-changes-better-in-contract-management/>

QUESTION NO: 231

The executive management team is mandating the company develop a disaster recovery plan. The cost must be kept to a minimum, and the money to fund additional internet connections is not available. Which of the following would be the **best** option?

- A.**
Hot site
- B.**
Cold site
- C.**
Failover site
- D.**
Warm site

Answer: B

Reference: <https://www.pslightwave.com/disaster-recovery-plans-three-site-strategies-you-should-consider/>

QUESTION NO: 232

An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?

- A.**
Deploy multifactor authentication.
- B.**
Decrease the level of the web filter settings.
- C.**
Implement security awareness training.
- D.**
Update the acceptable use policy.

Answer: C

Reference: <https://us.norton.com/blog/malware/website-spoofing>

QUESTION NO: 233

Which of the following teams is **best** suited to determine whether a company has systems that can be exploited by a potential, identified vulnerability?

- A.**
Purple team
- B.**
Blue team
- C.**
Red team
- D.**
White team

Answer: C

Reference: <https://www.ibm.com/topics/penetration-testing>

QUESTION NO: 234

A company is reviewing options to enforce user logins after several account takeovers. The following conditions must be met as part of the solution:

- Allow employees to work remotely or from assigned offices around the world.
- Provide a seamless login experience.
- Limit the amount of equipment required.

Which of the following **best** meets these conditions?

- A.**
Trusted devices

- B.**
Geotagging
- C.**
Smart cards
- D.**
Time-based logins

Answer: A

Reference: <https://techcommunity.microsoft.com/t5/microsoft-365-blog/enable-a-seamless-remote-work-experience-for-your-users/ba-p/1673025>

QUESTION NO: 235

Which of the following methods can be used to detect attackers who have successfully infiltrated a network? (Choose two.)

- A.**
Tokenization
- B.**
CI/CD
- C.**
Honeypots
- D.**
Threat modeling
- E.**
DNS sinkhole
- F.**
Data obfuscation

Answer: C,E

Reference: <https://cyberthreatportal.com/types-of-network-attacks-and-prevention/>

QUESTION NO: 236

A company wants to ensure that the software it develops will not be tampered with after the final version is completed. Which of the following should the company **most** likely use?

- A.
Hashing
- B.
Encryption
- C.
Baselines
- D.
Tokenization

Answer: A

Reference: <https://www.securityscientist.net/blog/protect-all-forms-of-code-from-unauthorized-access-and-tampering-6-practices/>

QUESTION NO: 237

An organization completed a project to deploy SSO across all business applications last year. Recently, the finance department selected a new cloud-based accounting software vendor. Which of the following should **most** likely be configured during the new software deployment?

- A.
RADIUS
- B.
SAML
- C.
EAP
- D.
OpenID

Answer: B

Reference: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/add-application-portal-setup-sso>

QUESTION NO: 238

A user, who is waiting for a flight at an airport, logs in to the airline website using the public Wi-Fi, ignores a security warning and purchases an upgraded seat. When the flight lands, the user finds unauthorized credit card charges. Which of the following attacks **most** likely occurred?

- A.**
Replay attack
- B.**
Memory leak
- C.**
Buffer overflow attack
- D.**
On-path attack

Answer: D

Reference: <https://securityaffairs.com/159003/security/public-wi-fi-attacks.html>

QUESTION NO: 239

A network engineer deployed a redundant switch stack to increase system availability. However, the budget can only cover the cost of one ISP connection. Which of the following **best** describes the potential risk factor?

- A.**
The equipment MTBF is unknown.
- B.**
The ISP has no SLA.
- C.**
An RPO has not been determined.
- D.**
There is a single point of failure.

Answer: D

Reference: <https://www.lancom-systems.com/fileadmin/download/techpaper/LANCOM-Techpaper-Switch-design-guide-redundancy-concepts.pdf>

QUESTION NO: 240

A network team segmented a critical, end-of-life server to a VLAN that can only be reached by specific devices but cannot be reached by the perimeter network. Which of the following **best** describe the controls the team implemented? (Choose two.)

- A.**
Managerial
- B.**
Physical
- C.**
Corrective
- D.**
Detective
- E.**
Compensating
- F.**
Technical
- G.**
Deterrent

Answer: E,F

Reference:

https://www.adventuresinsecurity.com/Files/VLAN_network_segmentation_and_security.pdf

QUESTION NO: 241

A threat actor was able to use a username and password to log in to a stolen company mobile device. Which of the following provides the **best** solution to increase mobile data security on all employees' company mobile devices?

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

Answer: D

Reference: <https://brightsec.com/blog/mobile-security-6-ways-to-protect-mobile-devices/>

QUESTION NO: 242

Which of the following **best** describes the risk present after controls and mitigating factors have been applied?

- A.
Residual
- B.
Avoided
- C.
Inherent
- D.
Operational

Answer: A

Reference: <https://linfordco.com/blog/linking-monitoring-risks-controls/>

QUESTION NO: 243

A software development team asked a security administrator to recommend techniques that should be used to reduce the chances of the software being reverse engineered. Which of the

following should the security administrator recommend?

- A.**
Digitally signing the software
- B.**
Performing code obfuscation
- C.**
Limiting the use of third-party libraries
- D.**
Using compile flags

Answer: B

Reference: <https://www.sofpro.com/blog/software-reverse-engineering-protection>

QUESTION NO: 244

Which of the following is a possible factor for MFA?

- A.**
Something you exhibit
- B.**
Something you have
- C.**
Somewhere you are
- D.**
Someone you know

Answer: B

Reference: <https://jumpcloud.com/blog/different-factors-of-multi-factor-authentication-mfa>

QUESTION NO: 245

Easy-to-guess passwords led to an account compromise. The current password policy requires at least 12 alphanumeric characters, one uppercase character, one lowercase character, a password history of two passwords, a minimum password age of one day, and a maximum password age of 90 days. Which of the following would reduce the risk of this incident from happening again? (Choose two.)

A.

Increasing the minimum password length to 14 characters.

B.

Upgrading the password hashing algorithm from MD5 to SHA-512.

C.

Increasing the maximum password age to 120 days.

D.

Reducing the minimum password length to ten characters.

E.

Reducing the minimum password age to zero days.

F.

Including a requirement for at least one special character.

Answer: A,F

Reference: <https://www.infosecurity-magazine.com/news-features/reduce-risk-password-compromise/>

QUESTION NO: 246

A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the **most** likely explanation of this unauthorized connection?

A.

The software had a hidden keylogger.

B.

The software was ransomware.

C.

The user's computer had a fileless virus.

D.

The software contained a backdoor.

Answer: D

Reference: <https://support.microsoft.com/en-us/windows/protect-your-pc-from-potentially-unwanted-applications-c7668a25-174e-3b78-0191-faf0607f7a6e>

QUESTION NO: 247

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:

A starting baseline of 50% memory utilization

Storage scalability

Single circuit failure resilience

Which of the following **best** meets all of these requirements?

A.

Connecting dual PDUs to redundant power supplies

B.

Transitioning the platform to an IaaS provider

C.

Configuring network load balancing for multiple paths

D.

Deploying multiple large NAS devices for each host

Answer: B

Reference: <https://www.lucidchart.com/blog/reliability-availability-in-cloud-computing>

QUESTION NO: 248

Which of the following **best** describes a use case for a DNS sinkhole?

"Everything is under control" - www.pass4sure.com

A.

Attackers can see a DNS sinkhole as a highly valuable resource to identify a company's domain structure.

B.

A DNS sinkhole can be used to draw employees away from known-good websites to malicious ones owned by the attacker.

C.

A DNS sinkhole can be used to capture traffic to known-malicious domains used by attackers.

D.

A DNS sinkhole can be set up to attract potential attackers away from a company's network resources.

Answer: C

Reference: <https://bluecatnetworks.com/blog/dns-sinkhole-a-tool-to-help-thwart-cyberattacks/>

QUESTION NO: 249

An incident analyst finds several image files on a hard disk. The image files may contain geolocation coordinates. Which of the following **best** describes the type of information the analyst is trying to extract from the image files?

A.

Log data

B.

Metadata

C.

Encrypted data

D.

Sensitive data

Answer: B

Reference: <https://products.aspose.app/gis/geotag-photo>

QUESTION NO: 250

Which of the following **most** likely describes why a security engineer would configure all outbound emails to use S/MIME digital signatures?

- A.**
To meet compliance standards
- B.**
To increase delivery rates
- C.**
To block phishing attacks
- D.**
To ensure non-repudiation

Answer: D

Reference: <https://www.digicert.com/faq/email-trust/what-is-smime-or-encrypted-email>

QUESTION NO: 251

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

- A.**
Whaling
- B.**
Credential harvesting
- C.**
Prepending
- D.**
Dumpster diving

Answer: D

Reference: <https://www.imgsecurity.com/how-criminals-are-hacking-printers-to-take-over-your-entire-network/>

QUESTION NO: 252

Which of the following considerations is the **most** important regarding cryptography used in an IoT device?

- A.**
Resource constraints
- B.**
Available bandwidth
- C.**
The use of block ciphers
- D.**
The compatibility of the TLS version

Answer: A

Reference: <https://www.geeksforgeeks.org/cryptography-in-iot-internet-of-things/>

QUESTION NO: 253

A coffee shop owner wants to restrict internet access to only paying customers by prompting them for a receipt number. Which of the following is the **best** method to use given this requirement?

- A.**
WPA3
- B.**
Captive portal
- C.**
PSK
- D.**
IEEE 802.1X

Answer: B

Reference: <https://superuser.com/questions/452147/how-do-i-restrict-or-block-internet-access-on-a-home-network>

QUESTION NO: 254

While performing digital forensics, which of the following is considered the **most** volatile and should have the contents collected **first**?

- A.**
Hard drive
- B.**
RAM
- C.**
SSD
- D.**
Temporary files

Answer: B

Reference: <https://link.springer.com/article/10.1007/s11276-020-02535-5>

QUESTION NO: 255

A hosting provider needs to prove that its security controls have been in place over the last six months and have sufficiently protected customer data. Which of the following would provide the **best** proof that the hosting provider has met the requirements?

- A.**
NIST CSF
- B.**
SOC 2 Type 2 report
- C.**
CIS Top 20 compliance reports
- D.**
Vulnerability report

Answer: B

Reference: <https://www.cloudpanel.io/blog/web-hosting-security/>

QUESTION NO: 256

A city municipality lost its primary data center when a tornado hit the facility. Which of the following should the city staff use immediately after the disaster to handle essential public services?

- A.**
BCP
- B.**
Communication plan
- C.**
DRP
- D.**
IRP

Answer: C

Reference: <https://linfordco.com/blog/bcp-vs-drp/>

QUESTION NO: 257

Which of the following is considered a preventive control?

- A.**
Configuration auditing
- B.**
Log correlation
- C.**
Incident alerts
- D.**
Segregation of duties

Answer: D

Reference: <https://community.trustcloud.ai/docs/grc-launchpad/grc-101/compliance/corrective-control-building-a-resilient-security-posture/>

QUESTION NO: 258

A systems administrator notices that a testing system is down. While investigating, the systems administrator finds that the servers are online and accessible from any device on the server network. The administrator reviews the following information from the monitoring system:

Server name	IP	Traffic sent	Traffic received	Status
File01	10.12.14.13	2654812	23185	Up
DC01	10.12.15.2	168741	65481	Up
Test01	10.25.1.3	14872	654123168	Down
Test02	10.25.1.4	16941	651321685	Down
DC02	10.12.15.3	32145	32158	Up
Finance01	10.18.1.14	12374	6548	Up

Which of the following is the **most** likely cause of the outage?

- A.**
Denial of service
- B.**
ARP poisoning
- C.**
Jamming
- D.**
Kerberoasting

Answer: D

QUESTION NO: 259

A security team has been alerted to a flood of incoming emails that have various subject lines and are addressed to multiple email inboxes. Each email contains a URL shortener link that is redirecting to a dead domain. Which of the following is the **best** step for the security team to take?

- A.**
Create a blocklist for all subject lines.
- B.**
Send the dead domain to a DNS sinkhole.
- C.**
Quarantine all emails received and notify all employees.
- D.**
Block the URL shortener domain in the web proxy.

Answer: B

QUESTION NO: 260

A security administrator is working to secure company data on corporate laptops in case the laptops are stolen. Which of the following solutions should the administrator consider?

- A.**
Disk encryption
- B.**
Data loss prevention
- C.**
Operating system hardening
- D.**
Boot security

Answer: A

Reference: <https://www.aegisifs.com/blog/how-protect-company-laptops-and-their-data>

QUESTION NO: 261

A company needs to keep the fewest records possible, meet compliance needs, and ensure destruction of records that are no longer needed. Which of the following **best** describes the policy that meets these requirements?

- A.**

Security policy

B.

Classification policy

C.

Retention policy

D.

Access control policy

Answer: C

Reference: <https://www.workstream.us/policy-templates/record-retention-policy>

QUESTION NO: 262

Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A.

Code repositories

B.

Dark web

C.

Threat feeds

D.

State actors

E.

Vulnerability databases

Answer: A

Reference: <https://securityboulevard.com/2021/07/reducing-the-risk-of-credential-leakage/>

QUESTION NO: 263

Which of the following is the **best** reason an organization should enforce a data classification policy to help protect its most sensitive information?

- A.**
End users will be required to consider the classification of data that can be used in documents.
- B.**
The policy will result in the creation of access levels for each level of classification.
- C.**
The organization will have the ability to create security requirements based on classification levels.
- D.**
Security analysts will be able to see the classification of data within a document before opening it.

Answer: C

Reference: <https://convergetp.com/2024/02/13/data-classification-security-strategy/>

QUESTION NO: 264

An analyst is performing a vulnerability scan against the web servers exposed to the internet without a system account. Which of the following is **most** likely being performed?

- A.**
Non-credentialed scan
- B.**
Packet capture
- C.**
Privilege escalation
- D.**
System enumeration
- E.**
Passive scan

Answer: A

Reference: <https://beaglesecurity.com/blog/article/authenticated-vs-unauthenticated-scans.html>

QUESTION NO: 265

A security administrator is hardening corporate systems and applying appropriate mitigations by consulting a real-world knowledge base for adversary behavior. Which of the following would be **best** for the administrator to reference?

- A.**
MITRE ATT&CK
- B.**
CSIRT
- C.**
CVSS
- D.**
SOAR

Answer: A

Reference: <https://attack.mitre.org/>

QUESTION NO: 266

An architect has a request to increase the speed of data transfer using JSON requests externally. Currently, the organization uses SFTP to transfer data files. Which of the following will **most** likely meet the requirements?

- A.**
A website-hosted solution
- B.**
Cloud shared storage
- C.**
A secure email solution
- D.**
Microservices using API

Answer: D

QUESTION NO: 267

Which of the following addresses individual rights such as the right to be informed, the right of access, and the right to be forgotten?

- A.**
GDPR
- B.**
PCI DSS
- C.**
NIST
- D.**
ISO

Answer: A

Reference: <https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

QUESTION NO: 268

An administrator is installing an LDAP browser tool in order to view objects in the corporate LDAP directory. Secure connections to the LDAP server are required. When the browser connects to the server, certificate errors are being displayed, and then the connection is terminated. Which of the following is the most likely solution?

- A.**
The administrator should allow SAN certificates in the browser configuration.
- B.**
The administrator needs to install the server certificate into the local truststore.
- C.**
The administrator should request that the secure LDAP port be opened to the server.
- D.**
The administrator needs to increase the TLS version on the organization's RA.

Answer: B

QUESTION NO: 269

Which of the following is the **most** important security concern when using legacy systems to provide production service?

- A.**
Instability
- B.**
Lack of vendor support
- C.**
Loss of availability
- D.**
Use of insecure protocols

Answer: B

Reference: <https://nquirminds.com/cybernews/the-risks-and-challenges-of-legacy-systems-in-cybersecurity/>

QUESTION NO: 270

A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following **most** likely occurred?

- A.**
A spraying attack was used to determine which credentials to use.
- B.**
A packet capture tool was used to steal the password.
- C.**
A remote-access Trojan was used to install the malware.
- D.**
A dictionary attack was used to log in as the server administrator.

Answer: B

QUESTION NO: 271

A user is requesting Telnet access to manage a remote development web server. Insecure protocols are not allowed for use within any environment. Which of the following should be configured to allow remote access to this server?

- A.**
HTTPS
- B.**
SNMPv3
- C.**
SSH
- D.**
RDP
- E.**
SMTP

Answer: C

Reference: <https://www.cloudflare.com/learning/access-management/what-is-ssh/>

QUESTION NO: 272

A security administrator is working to find a cost-effective solution to implement certificates for a large number of domains and subdomains owned by the company. Which of the following types of certificates should the administrator implement?

- A.**
Wildcard
- B.**
Client certificate
- C.**
Self-signed
- D.**
Code signing

Answer: A

QUESTION NO: 273

An auditor discovered multiple insecure ports on some servers. Other servers were found to have legacy protocols enabled. Which of the following tools did the auditor use to discover these issues?

- A.**
Nessus
- B.**
curl
- C.**
Wireshark
- D.**
netcat

Answer: A

Reference: <https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-insecure-protocols-workbook-implementation-guide/ba-p/1197564>

QUESTION NO: 274

A security analyst received a tip that sensitive proprietary information was leaked to the public. The analyst is reviewing the PCAP and notices traffic between an internal server and an external host that includes the following:

...

```
12:47:22.327233 PPPoE [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41),  
length 331) 10.5.1.1 > 52.165.16.154: IP6 (hlim E3, next-header TCP (6) payload length: 271)  
2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:dddd:a601:24fa.13788: Flags [P.],  
cksum 0xd7ee (correct), seq 97:348, ack 102, win 16444, length 251
```

...

Which of the following was most likely used to exfiltrate the data?

- A.**
Encapsulation
- B.**
MAC address spoofing
- C.**
Steganography
- D.**
Broken encryption
- E.**
Sniffing via on-path position

Answer: A

QUESTION NO: 275

A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

- A.**
Serverless architecture
- B.**
Thin clients
- C.**
Private cloud
- D.**
Virtual machines

Answer: A

QUESTION NO: 276

A security administrator is performing an audit on a stand-alone UNIX server, and the following message is immediately displayed:

(Error 13): /etc/shadow: Permission denied.

Which of the following **best** describes the type of tool that is being used?

- A.
Pass-the-hash monitor
- B.
File integrity monitor
- C.
Forensic analysis
- D.
Password cracker

Answer: B

QUESTION NO: 277

A security administrator needs to create firewall rules for the following protocols: RTP, SIP, H.323, and SRTP. Which of the following does this rule set support?

- A.
RTOS
- B.
VoIP
- C.
SoC
- D.
HVAC

Answer: B

QUESTION NO: 278

Which of the following **best** describes a social engineering attack that uses a targeted electronic messaging campaign aimed at a Chief Executive Officer?

- A.
Whaling

- B.**
Spear phishing
- C.**
Impersonation
- D.**
Identity fraud

Answer: A

QUESTION NO: 279

During a penetration test, a flaw in the internal PKI was exploited to gain domain administrator rights using specially crafted certificates. Which of the following remediation tasks should be completed as part of the cleanup phase?

- A.**
Updating the CRL
- B.**
Patching the CA
- C.**
Changing passwords
- D.**
Implementing SOAR

Answer: A

QUESTION NO: 280

A company wants to implement MFA. Which of the following enables the additional factor while using a smart card?

- A.**
PIN
- B.**
Hardware token
- C.**

User ID

D.
SMS

Answer: A

Reference: <https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf>

QUESTION NO: 281

A company hired an external consultant to assist with required system upgrades to a critical business application. A systems administrator needs to secure the consultant's access without sharing passwords to critical systems. Which of the following solutions should **most** likely be utilized?

A.
TACACS+

B.
SAML

C.
An SSO platform

D.
Role-based access control

E.
PAM software

Answer: E

QUESTION NO: 282

A newly implemented wireless network is designed so that visitors can connect to the wireless network for business activities. The legal department is concerned that visitors might connect to the network and perform illicit activities. Which of the following should the security team implement to address this concern?

A.

Configure a RADIUS server to manage device authentication.

B.

Use 802.1X on all devices connecting to wireless.

C.

Add a guest captive portal requiring visitors to accept terms and conditions.

D.

Allow for new devices to be connected via WPS.

Answer: C

QUESTION NO: 283

Which of the following data roles is responsible for identifying risks and appropriate access to data?

A.

Owner

B.

Custodian

C.

Steward

D.

Controller

Answer: A

Reference: <https://dainstudios.com/insights/data-governance-roles/>

QUESTION NO: 284

Which of the following physical controls can be used to **both** detect and deter? (Choose two.)

A.

Lighting

B.

Fencing

C.

Signage

D.

Sensor

E.

Bollard

F.

Lock

Answer: A,D

Reference: <https://www.securityscientist.net/blog/a-list-of-physical-controls-of-the-iso27002/>

QUESTION NO: 285

A multinational bank hosts several servers in its data center. These servers run a business-critical application used by customers to access their account information. Which of the following should the bank use to ensure accessibility during peak usage times?

A.

Load balancer

B.

Cloud backups

C.

Geographic dispersal

D.

Disk multipathing

Answer: A

Reference: <https://learn.microsoft.com/en-us/azure/well-architected/performance-efficiency/capacity-planning>

QUESTION NO: 286

The author of a software package is concerned about bad actors repackaging and inserting malware into the software. The software download is hosted on a website, and the author exclusively controls the website's contents. Which of the following techniques would **best** ensure the software's integrity?

- A.
Input validation
- B.
Code signing
- C.
Secure cookies
- D.
Fuzzing

Answer: B

Reference: <https://garantir.io/preventing-malware-injections/>

QUESTION NO: 287

A third-party vendor is moving a particular application to the end-of-life stage at the end of the current year. Which of the following is the **most** critical risk if the company chooses to continue running the application?

- A.
Lack of security updates
- B.
Lack of new features
- C.
Lack of support
- D.
Lack of source code access

Answer: A

Reference: <https://www.spiceworks.com/it-articles/end-of-life-software-dangers/>

QUESTION NO: 288

A security analyst recently read a report about a flaw in several of the organization's printer models that causes credentials to be sent over the network in cleartext, regardless of the encryption settings. Which of the following would be **best** to use to validate this finding?

- A.**
Wireshark
- B.**
netcat
- C.**
Nessus
- D.**
Nmap

Answer: A

Reference: <https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-clear-text>

QUESTION NO: 289

A development team is launching a new public-facing web product. The Chief Information Security Officer has asked that the product be protected from attackers who use malformed or invalid inputs to destabilize the system. Which of the following practices should the development team implement?

- A.**
Fuzzing
- B.**
Continuous deployment
- C.**
Static code analysis
- D.**
Manual peer review

Answer: A

Reference: <https://www.esecurityplanet.com/endpoint/prevent-web-attacks-using-input-sanitization/>

QUESTION NO: 290

During an annual review of the system design, an engineer identified a few issues with the currently released design. Which of the following should be performed **next** according to best practices?

- A.**
Risk management process
- B.**
Product design process
- C.**
Design review process
- D.**
Change control process

Answer: C

Reference: <https://www.codingdrills.com/tutorial/system-design-tutorial/design-process>

QUESTION NO: 291

Which of the following is **best** to use when determining the severity of a vulnerability?

- A.**
CVE
- B.**
OSINT
- C.**
SOAR
- D.**

CVSS

Answer: D

Reference: <https://nvd.nist.gov/vuln-metrics/cvss>

QUESTION NO: 292

An organization experienced a security breach that allowed an attacker to send fraudulent wire transfers from a hardened PC exclusively to the attacker's bank through remote connections. A security analyst is creating a timeline of events and has found a different PC on the network containing malware. Upon reviewing the command history, the analyst finds the following:

```
PS>.\mimikatz.exe "sekurlsa::pth /user:localadmin /domain:corp-domain.com  
/ntlm:B4B9B02E1F29A3CF193EAB28C8D617D3F327
```

Which of the following **best** describes how the attacker gained access to the hardened PC?

- A.**
The attacker created fileless malware that was hosted by the banking platform.
- B.**
The attacker performed a pass-the-hash attack using a shared support account.
- C.**
The attacker utilized living-off-the-land binaries to evade endpoint detection and response software.
- D.**
The attacker socially engineered the accountant into performing bad transfers.

Answer: B

Reference: <https://blog.netwrix.com/2021/11/30/passing-the-hash-with-mimikatz/>

QUESTION NO: 293

Which of the following is the **best** resource to consult for information on the most common application exploitation methods?

- A.
OWASP
- B.
STIX
- C.
OVAL
- D.
Threat intelligence feed
- E.
Common Vulnerabilities and Exposures

Answer: A

Reference: <https://owasp.org/www-project-top-ten/>

QUESTION NO: 294

A security analyst is reviewing the logs on an organization's DNS server and notices the following unusual snippet:

```
Log from named: post-processed 20230102 0045L
...
qry_source: 124.22.158.37 TCP/53
qry_dest: 52.165.16.154 TCP/53
qry_dest: 10.100.50.5 TCP/53
qry_type: AXFR
| zone int.comptia.org
-----| www A 10.100.50.21
-----| dns A 10.100.5.5
-----| adds A 10.101.10.10
-----| fshare A 10.101.10.20
-----| sip A 10.100.5.11
...
```

Which of the following attack techniques was **most** likely used?

- A.**
Determining the organization's ISP-assigned address space
- B.**
Bypassing the organization's DNS sinkholing
- C.**
Footprinting the internal network
- D.**
Attempting to achieve initial access to the DNS server
- E.**
Exfiltrating data from fshare.int.complia.org

Answer: C

Reference: <https://www.acunetix.com/blog/articles/dns-zone-transfers-axfr/>

QUESTION NO: 295

A security analyst at an organization observed several user logins from outside the organization's network. The analyst determined that these logins were not performed by individuals within the organization. Which of the following recommendations would reduce the likelihood of future attacks? (Choose two.)

- A.**
Disciplinary actions for users
- B.**
Conditional access policies
- C.**
More regular account audits
- D.**
Implementation of additional authentication factors
- E.**
Enforcement of content filtering policies
- F.**
A review of user account permissions

Answer: B,D

Reference: <https://www.cynet.com/network-attacks/unauthorized-access-5-best-practices-to-avoid-the-next-data-breach/>

QUESTION NO: 296

A security team is addressing a risk associated with the attack surface of the organization's web application over port 443. Currently, no advanced network security capabilities are in place. Which of the following would be **best** to set up? (Choose two.)

- A.
NIDS
- B.
Honeypot
- C.
Certificate revocation list
- D.
HIPS
- E.
WAF
- F.
SIEM

Answer: E,F

Reference: <https://www.wordfence.com/blog/2022/06/securing-port-443/>

QUESTION NO: 297

A systems administrator would like to create a point-in-time backup of a virtual machine. Which of the following should the administrator use?

- A.
Replication

- B.**
Simulation
- C.**
Snapshot
- D.**
Containerization

Answer: C

Reference: <https://www.veeam.com/blog/best-way-backup-vmware.html>

QUESTION NO: 298

A security administrator notices numerous unused, non-compliant desktops are connected to the network. Which of the following actions would the administrator **most** likely recommend to the management team?

- A.**
Monitoring
- B.**
Decommissioning
- C.**
Patching
- D.**
Isolating

Answer: B

Reference: <https://www.businesstechweekly.com/cybersecurity/network-security/network-hardening/>

QUESTION NO: 299

Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?

- A.**
Sanitization
- B.**
Formatting
- C.**
Degaussing
- D.**
Defragmentation

Answer: A

Reference: <https://dzone.com/articles/how-to-erase-or-wipe-sensitive-files-from-hard-drive>

QUESTION NO: 300

An organization wants to improve the company's security authentication method for remote employees. Given the following requirements:

- Must work across SaaS and internal network applications
- Must be device manufacturer agnostic
- Must have offline capabilities

Which of the following would be the **most** appropriate authentication method?

- A.**
Username and password
- B.**
Biometrics
- C.**
SMS verification
- D.**
Time-based tokens

Answer: D

Reference: <https://workos.com/blog/saas-authentication>

QUESTION NO: 301

A security officer is implementing a security awareness program and has placed security-themed posters around the building and assigned online user training. Which of the following will the security officer **most** likely implement?

- A.**
Password policy
- B.**
Access badges
- C.**
Phishing campaign
- D.**
Risk assessment

Answer: C

Reference: <https://blog.rsisecurity.com/best-practices-for-implementing-a-security-awareness-program/>

QUESTION NO: 302

A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following **best** describes this type of vulnerability?

- A.**
DDoS attack
- B.**
Rogue employee
- C.**
Insider threat
- D.**
Supply chain

Answer: D

Reference: <https://www.crowdstrike.com/cybersecurity-101/types-of-cyber-vulnerabilities/>

QUESTION NO: 303

A company web server is initiating outbound traffic to a low-reputation, public IP on non-standard port. The web server is used to present an unauthenticated page to clients who upload images to the company. An analyst notices a suspicious process running on the server that was not created by the company development team. Which of the following is the **most** likely explanation for this security incident?

A.

A web shell has been deployed to the server through the page.

B.

A vulnerability has been exploited to deploy a worm to the server.

C.

Malicious insiders are using the server to mine cryptocurrency.

D.

Attackers have deployed a rootkit Trojan to the server over an exposed RDP port.

Answer: A

Reference: <https://serverfault.com/questions/443038/what-does-incoming-and-outgoing-traffic-mean>

QUESTION NO: 304

An organization requests a third-party full-spectrum analysis of its supply chain. Which of the following would the analysis team use to meet this requirement?

A.

Vulnerability scanner

B.

Penetration test

C.

SCAP

D.
Illumination tool

Answer: D

Reference: <https://theowlsolutions.com/third-party-supply-chain-analytics/>

QUESTION NO: 305

A systems administrator deployed a monitoring solution that does not require installation on the endpoints that the solution is monitoring. Which of the following is described in this scenario?

A.
Agentless solution

B.
Client-based soon

C.
Open port

D.
File-based solution

Answer: A

Reference: <https://www.strongdm.com/what-is/agentless-monitoring>

QUESTION NO: 306

A security analyst is reviewing the source code of an application in order to identify misconfigurations and vulnerabilities. Which of the following kinds of analysis best describes this review?

A.
Dynamic

B.
Static

C.
Gap

D.
Impact

Answer: B