DUMPSARENA

CompTIA Security+ Exam

CompTIA SY0-701

Version Demo

Total Demo Questions: 93

Total Premium Questions: 930

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, General Security Concepts	76
Topic 2, Threats, Vulnerabilities, and Mitigations	258
Topic 3, Security Architecture	217
Topic 4, Security Operations	153
Topic 5, Security Program Management and Oversight	225
Total	930

QUESTION NO: 1

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

Explanation:

Asset stickers tied to employee IDs make ownership and responsibility crystal clear. If a laptop gets flagged for malware, suspicious logins, or it simply goes missing, the security team doesn't have to guess who had it last—they can quickly identify the right person and respond faster. That speed matters when you're trying to contain an incident and reduce damage.

This also helps a lot during offboarding. When someone leaves, you want to be sure the correct laptop is returned and that company data is handled properly (backed up if needed, then wiped, reimaged, or otherwise secured). Good asset tracking supports that chain of custody and reduces the chance that sensitive data walks out the door with an unreturned device.

The other choices sound security-related, but they don't really depend on physical asset stickers. Things like MFA token setup, firewall targeting, penetration testing, and training distribution are typically driven by directory accounts, device management tools, hostnames, certificates, or IP/MAC info—not a sticker number.

References: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final and https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

QUESTION NO: 2

Which of the following are the first steps an analyst should perform when developing a heat map? (Choose two.)

A. Methodically walk around the office noting Wi-Fi signal strength.

B. Log in to each access point and check the settings.

C. Create or obtain a layout of the office.

D. Measure cable lengths between access points.

E. Review access logs to determine the most active devices.

F. Remove possible impediments to radio transmissions.

ANSWER: A C

Explanation:

To build a Wi-Fi heat map, you start with two basics: a floor plan and real signal measurements. Getting or creating an office layout gives you the "canvas" you'll map coverage onto—without it, the results don't mean much because you can't tie signal levels to specific rooms, walls, or problem areas.

Next, you do a site walk (or survey) and record signal strength at different spots. That's how the heat map is actually formed: it's based on measured RF data (RSSI/SNR) taken around the space. You can do this with a survey tool and a laptop/phone, but the key idea is physically moving through the area and collecting readings.

The other choices aren't really first steps for a heat map. Logging into APs and checking settings can help later with tuning, and access logs tell you usage patterns, not coverage. Measuring cable lengths is unrelated. Removing impediments might be a possible remediation step, but you don't start by changing the environment before you've measured and mapped the current state.

References: https://www.cisco.com/c/en/us/products/wireless/wireless-site-survey.html and https://www.netspotapp.com/wifi-heatmap.html

QUESTION NO: 3

An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?

A. Side loading

B. Target of evaluation

C. Resource reuse

D. SQL injection

ANSWER: D

Explanation:

This is describing an injection-style attack: the attacker is deliberately sending "weird" or unexpected characters (like quotes, semicolons, comment markers, etc.) to change how the backend interprets a request. When the target is a database query, that technique is most commonly known as SQL injection.

With SQL injection, the attacker tries to trick the application into running extra SQL commands, or altering the logic of a query, so they can read data they shouldn't (like user records), bypass logins, or even modify database content. The key clue in the question is "unexpected characters" used to access "information within the underlying systems," which fits SQLi very well.

The other options don't match: side loading is about loading a malicious DLL/app in place of a legitimate one, "target of evaluation" is a security evaluation term, and resource reuse is about reusing objects/resources in an unsafe way. For a quick overview of SQL injection and why it works, see https://owasp.org/www-community/attacks/SQL_Injection and https://www.cisa.gov/news-events/news/understanding-sql-injection.

QUESTION NO: 4

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Select 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: C E

Explanation:

The two big things you want nailed down in a security awareness curriculum are: what you're training people to defend against, and how often you're going to reinforce it. If you don't tailor training to the real threat vectors in your industry (phishing, ransomware, BEC, data handling risks, etc.), the program turns into generic "check-the-box" content that employees won't connect to their day-to-day work.

The other key piece is cadence and duration. People forget security lessons fast if they only hear them once a year, but they'll also tune out if sessions are too long or too frequent. A good plan balances short, repeatable touchpoints (like quick modules, newsletters, or mini-quizzes) with occasional deeper training, so the message sticks without burning everyone out.

Other options listed can be useful in a broader program, but they're not the core "curriculum planning" priorities. For example, secure software development training is important, but it's role-based—not for all personnel. Retraining after phishing failures is more of an operational follow-up control than a primary curriculum design factor.

References: https://www.nist.gov/privacy-framework/nist-sp-800-50-building-information-technology-security-awareness-and-training-program and https://www.cisa.gov/resources-tools/resources/security-awareness-toolkit

QUESTION NO: 5

Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Choose two.)

A. Easier debugging of the system

B. Reduced cost of ownership of the system

C. Improved scalability of the system

D. Increased compartmentalization of the system

E. Stronger authentication of the system

F. Reduced complexity of the system

ANSWER: C D

Explanation:

Microservices usually shine when it comes to **scaling**. Instead of scaling the whole app (like you often do with a monolith), you can scale only the service that's under pressure—say, the checkout service during a sale—without throwing extra resources at everything else. That's why "improved scalability" is a classic microservices benefit.

They also bring better **compartmentalization** (isolation). Each service is its own small unit, often with its own codebase and deployment. If one service has an issue or gets compromised, it's less likely to automatically take down the entire application. That separation can limit blast radius and makes it easier to apply targeted security controls and updates per service.

The other options sound nice, but they're not guaranteed. Debugging can actually get harder because requests hop across multiple services, ownership cost can go up due to added infrastructure/monitoring, and complexity often increases (distributed systems are tricky). Authentication isn't inherently stronger either—you still have to design it well.

References: https://microservices.io/ and https://www.ibm.com/topics/microservices

QUESTION NO: 6

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

Explanation:

A “deny any” rule at the bottom is a common best practice, but it’s also the kind of change that can break things fast if you missed even one needed “allow” rule above it. Firewalls and ACLs are processed top-to-bottom, so anything that isn’t explicitly permitted earlier will get dropped by that final deny—like management traffic, monitoring, backups, or even normal app ports to those servers.

The best way to prevent an outage like this is to test the rule change in a non-production (staging/lab) environment first. That gives you a safe place to confirm all the required traffic still works, spot what gets blocked, and adjust the allow rules before users and servers are impacted. It’s basically a rehearsal for the real network.

Change requests (A) are good process, but paperwork doesn’t stop a bad rule from blocking traffic. IPS signatures (C) aren’t the root problem here. And adding “allow any” above “deny any” (D) defeats the whole purpose of having a deny-all baseline.

References: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final, https://www.sans.org/white-papers/firewall-management/

QUESTION NO: 7

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head

B. Tcpdump

C. grep

D. rail

E. curl

F. openssi

G. dd

ANSWER: A C

Explanation:

head is perfect when you just want to quickly peek at the beginning of a big capture output file. Instead of opening the whole thing in an editor or scrolling forever, you can instantly view the first few lines (or first N lines) to confirm the earliest SOAP HTTP transactions look right.

For searching through the entire file for a specific word, header, or SOAP tag, **grep** is the go-to tool. It's fast, simple, and made for scanning large text files to find matching strings (and you can use options like case-insensitive search or showing line numbers if needed).

The other options don't fit as well: **tcpdump** is for capturing packets, not quickly reviewing the start of an already-saved text output; **curl** is for making HTTP requests; and tools like **dd** are for raw copying rather than readable review or string searching.

References: https://man7.org/linux/man-pages/man1/head.1.html and https://man7.org/linux/man-pages/man1/grep.1.html

QUESTION NO: 8

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? (Select two).

A. Federation

B. Identity proofing

C. Password complexity

D. Default password changes

E. Password manager

F. Open authentication

ANSWER: A C

Explanation:

The password rules (length, letters, numbers, and special characters) are a classic example of **password complexity**. That's simply the company enforcing a stronger password policy so accounts are harder to guess or crack with brute force.

The second part describes using the intranet account as the "main" identity to reach other company sites without creating separate logins everywhere. That's **federation** (often implemented as SSO), where one trusted identity is used to access multiple related services based on the user's profile/claims.

Options like identity proofing and default password changes can be part of onboarding, but they don't explain the "access multiple sites based on the intranet profile" piece. "Open authentication" (OAuth) is more about delegated authorization (letting an app access data) than logging into multiple internal sites using a central identity, so it's not the best fit here.

References: https://www.cloudflare.com/learning/access-management/what-is-federation/ and https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/passwords

QUESTION NO: 9

An administrator wants to automate an account permissions update for a large number of accounts. Which of the following would best accomplish this task?

A. Security groups

B. Federation

C. User provisioning

D. Vertical scaling

ANSWER: C

Explanation:

Correct answer: C. User provisioning

If you need to automate permission updates for lots of accounts at once, user provisioning is the best fit. Provisioning tools (often tied to IAM systems) are designed to automatically create, modify, and remove user access based on rules—like job role changes, department moves, or HR updates. That means you can push the same permission change across hundreds or thousands of accounts without touching each one manually.

Security groups can help standardize access, but they don't inherently "automate" updates across accounts unless you're also using an automated provisioning process to manage group membership. Federation is more about single sign-on and trusting identities from another system, not bulk permission updates. Vertical scaling is a computing resource concept (adding CPU/RAM), so it doesn't apply to account permissions at all.

For more background on what user provisioning covers in identity and access management, see: https://www.okta.com/identity-101/what-is-user-provisioning/ and https://learn.microsoft.com/en-us/entra/identity/app-provisioning/user-provisioning.

QUESTION NO: 10

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

Explanation:

You'd recommend decommissioning when the device can't be secured to the level your organization requires. If a device's encryption capabilities can't meet your standards (like not supporting modern TLS versions or strong ciphers), it's basically a permanent weak spot. You can try compensating controls, but at some point it's safer and cheaper to retire it than to keep building workarounds around it.

Another clear trigger is when the device can't receive authorized updates anymore. If the vendor has ended support or the hardware/software can't take signed firmware updates, you're stuck with known vulnerabilities and no clean way to patch them. That's a big risk, especially for network gear that sits in the middle of traffic.

The other choices (moving to test, relocating, or isolating it) don't automatically mean the device is unsafe—those are environment changes, not end-of-life reasons. Cleartext passwords are a serious issue, but it's usually a configuration problem you fix (disable telnet, use SSH, enforce strong auth) rather than immediately decommissioning the device.

References: https://www.cisa.gov/news-events/alerts/2019/10/03/alert-continued-threat-activity-targeting-network-infrastructure-devices and https://www.ncsc.gov.uk/collection/device-security-guidance

QUESTION NO: 11

An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?

A. Zero-day attacks

B. Insider threats

C. End-of-life support

D. Known exploits

ANSWER: D

Explanation:

Keeping network gear on the latest OS, patching servers, and updating endpoint definitions is basically classic “stay current” hygiene. That stuff is aimed at closing security holes we already know about—like vulnerabilities that have published CVEs and vendor fixes available. When you patch and update, you’re removing the easy paths attackers use when they rely on old, unpatched systems.

This won’t do much against a true zero-day, because by definition there’s no patch yet and signatures may not exist. It also doesn’t really stop insider threats, since insiders abuse legitimate access rather than missing patches. And “end-of-life support” isn’t an attack type—it’s more of a risk condition where you can’t get updates anymore.

So the best answer is that these actions most effectively prevent known exploits—things attackers can reliably target because they’re well-documented and commonly scanned for. References: https://www.cisa.gov/known-exploited-vulnerabilities-catalog and https://nvd.nist.gov/

QUESTION NO: 12

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

Explanation:

To get solid details about an executable running on a laptop, you want endpoint logs (usually from EDR). Endpoint telemetry is built for exactly this: it can show process creation events, the full path to the binary, parent/child process relationships, command-line arguments, file hashes, and even what network connections that specific process opened.

Network logs and IPS/IDS logs are great for spotting suspicious traffic patterns, ports, and destinations, but they typically won’t tell you which exact process on the laptop generated the traffic. Application logs can help if you already know which app is involved, but they’re usually not as reliable for deep process-level investigation.

So if the goal is “tell me more about the executable,” endpoint/EDR logs are the most direct and useful source. References: https://www.crowdstrike.com/cybersecurity-101/endpoint-detection-response-edr/ and https://learn.microsoft.com/en-us/defender-endpoint/overview-endpoint-detection-response

QUESTION NO: 13 - (SIMULATION)

SIMULATION

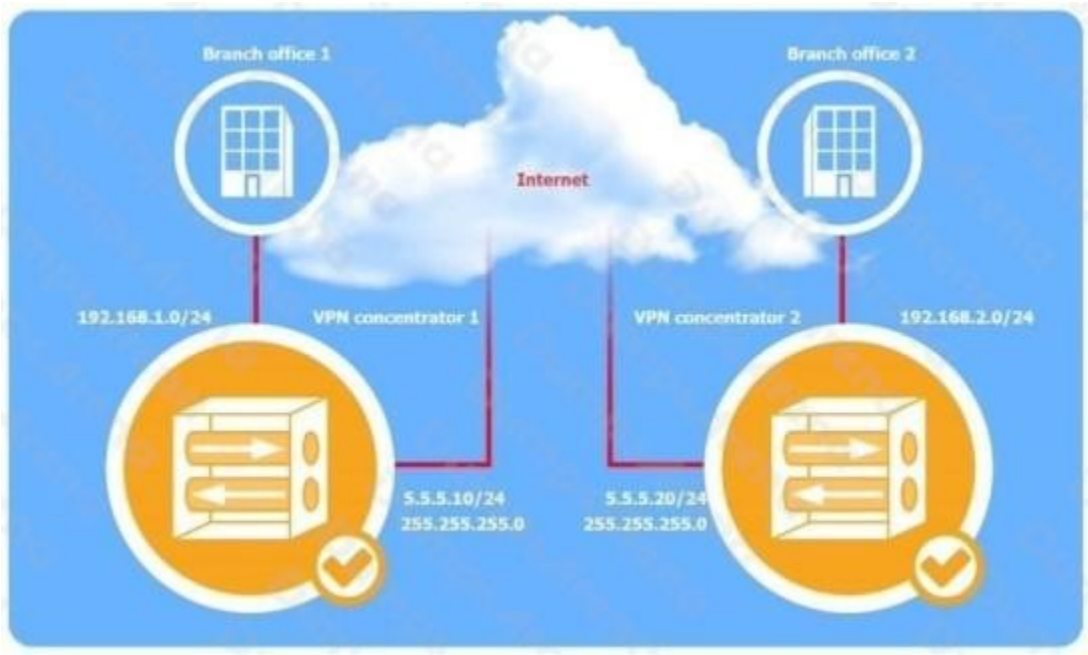
A systems administrator is configuring a site-to-site VPN between two branch offices. Some of the settings have already been configured correctly. The systems administrator has been provided the following requirements as part of completing the configuration:

• Most secure algorithms should be selected

• All traffic should be encrypted over the VPN

• A secret password will be used to authenticate the two VPN concentrators INSTRUCTIONS

Click on the two VPN Concentrators to configure the appropriate settings.



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

A. See Explanation section for answer.

ANSWER: See the explanation for the answer

Explanation:

QUESTION NO: 14

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

Explanation:

The two best fixes here are making passwords longer and expanding the allowed character set. Bumping the minimum length from 12 to 14 characters (A) helps a lot because length is what really drives password strength—each extra character massively increases the number of possible combinations, which makes guessing and cracking attempts much harder.

Adding a requirement for at least one special character (F) also helps reduce “easy-to-guess” patterns. If users are stuck with only letters and numbers, they tend to pick predictable stuff (names, seasons, simple swaps like Password12). Requiring a symbol pushes passwords away from those common patterns and makes rule-based cracking less effective.

The other choices don’t directly solve the “easy-to-guess password” problem. Upgrading MD5 to SHA-512 (B) is about protecting stored passwords if a database is stolen, not about stopping users from choosing weak ones in the first place. Increasing max age (C) makes things worse by letting weak passwords live longer. Reducing minimum length (D) obviously weakens security, and setting minimum age to zero (E) can let people quickly cycle passwords to get back to an old favorite.

References: https://pages.nist.gov/800-63-3/sp800-63b.html and https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

QUESTION NO: 15

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

Explanation:

This setup is a **technical control** because it’s enforced using technology—VLAN segmentation, switch/router configs, and usually ACLs or firewall rules to limit who can talk to that server. Nothing about this is policy-only or physical; it’s all happening in the network gear.

It’s also a **compensating control** because the server is end-of-life, meaning you often can’t fully fix the real problem (missing patches, unsupported OS, known vulnerabilities). Since you can’t remediate it properly, you reduce the risk another way by shrinking the attack surface—keeping it off the perimeter network and only allowing a small set of trusted devices to reach it.

That’s why options like detective or corrective don’t fit as well here. The goal isn’t to detect an attack or recover after one—it’s to limit exposure up front.

References: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final and https://www.cisco.com/c/en/us/products/switches/what-is-a-vlan.html

QUESTION NO: 16

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

Explanation:

The best move here is installing endpoint management software on all systems. That kind of tool (often called endpoint management, UEM, or EDR depending on features) gives you a central place to track what's installed, what's changed, and whether systems are staying in compliance with your baseline. If someone sneaks in unauthorized software or changes critical settings, you can usually detect it quickly and alert on it.

The other options are either too narrow or focused on the wrong layer. Logging scheduled tasks helps with one persistence method, but it won't reliably catch all software installs or configuration drift. Monitoring all outbound traffic is more of a network monitoring/egress control strategy—it can be useful, but it doesn't directly confirm what changed on the endpoint. Blocking known bad signatures is also helpful, but signature-based controls miss new or "living off the land" changes and don't provide full configuration monitoring.

For more background, see NIST's overview of endpoint security concepts at https://www.nist.gov/cybersecurity and Microsoft's explanation of endpoint management at https://learn.microsoft.com/en-us/mem/.

QUESTION NO: 17

An organization is implementing a COPE mobile device management policy. Which of the following should the organization include in the COPE policy? (Choose two.)

A. Remote wiping of the device

B. Data encryption

C. Requiring passwords with eight characters

D. Data usage caps

E. Employee data ownership

F. Personal application store access

ANSWER: A B

Explanation:

COPE (Corporate-Owned, Personally Enabled) means the company owns the phone, but the employee can still use it for some personal stuff. Because the organization owns the device, the policy should clearly allow strong security controls that protect corporate data even if the phone is lost, stolen, or the employee leaves.

That's why **remote wiping** is a must. If the device disappears or needs to be decommissioned, IT can erase corporate data (or the whole device) to prevent a data leak. This is a standard MDM feature for corporate-owned devices. See: https://support.apple.com/guide/deployment/remote-wipe-dep0f84c4c1d/web

Data encryption is also a core COPE requirement. Encryption helps ensure that even if someone gets physical access to the phone or its storage, the data isn't readable without the proper credentials/keys. This is one of the simplest ways to reduce the impact of device theft. See: https://source.android.com/docs/security/features/encryption

QUESTION NO: 18

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

Explanation:

The phase where you review roles and responsibilities is **Preparation**. This is the “get ready before anything goes wrong” part of incident response. You’re making sure the team knows who’s on point, who escalates to management, who talks to legal/PR, and who’s doing the hands-on technical work.

If you wait until *Analysis* or *Recovery* to figure out who’s responsible for what, you’ll lose time and people will step on each other’s toes during a real incident. Preparation is where you set the playbook, confirm contacts, define communication paths, and make sure everyone understands their job before the pressure is on.

NIST lays this out clearly in its incident handling guide, which describes preparation as the stage for building capability, including assigning roles and responsibilities: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. A shorter, practical view is also covered in the SANS Incident Handler’s Handbook: https://www.sans.org/white-papers/incident-handlers-handbook/.

QUESTION NO: 19

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

Explanation:

This is **impersonation** because the attacker is pretending to be the payroll department (a trusted internal authority) to get the employee to comply. That “I’m payroll, verify your credentials” angle is classic social engineering: it leans on trust and urgency to make someone act without thinking.

It’s also **smishing**, since the message is delivered by SMS/text. Smishing is basically phishing over text messages, and credential “verification” requests are one of the most common ways attackers try to steal usernames and passwords.

The other choices don’t fit as well: **vishing** would be a phone call, **typosquatting** is about look-alike web domains, and **misinformation** is more about spreading false info broadly rather than directly tricking someone into handing over credentials. While you could argue it’s “phishing” in a general sense, the test usually wants the more specific term when it’s available—so smishing is the better pick here.

References: https://csrc.nist.gov/glossary/term/phishing and https://www.sans.org/cyber-security-glossary/smishing/

QUESTION NO: 20

Which of the following objectives is best achieved by a tabletop exercise?

A. Familiarizing participants with the incident response process

B. Deciding red and blue team rules of engagement

C. Quickly determining the impact of an actual security breach

D. Conducting multiple security investigations in parallel

ANSWER: A

Explanation:

A tabletop exercise is basically a “talk-through” of an incident scenario. The main goal isn’t to catch a real attacker or do hands-on forensics—it’s to make sure everyone understands the incident response plan, their role, and the flow of communication when something goes wrong.

Because it’s discussion-based, a tabletop is great for finding gaps like unclear escalation paths, missing contact info, or confusion over who makes key decisions. It helps teams get comfortable with the process before a real incident forces them to figure it out under pressure.

The other choices don’t fit as well. Rules of engagement are more of a planning task for red/blue team exercises. Determining the impact of an actual breach is something you do during a live incident, not a tabletop. And running multiple investigations in parallel is an operational capability you’d test with more hands-on drills, not a discussion exercise.

References: https://www.cisa.gov/resources-tools/resources/tabletop-exercise-packages and https://www.ready.gov/exercises

QUESTION NO: 21

Which of the following would be indicative of a hidden audio le found inside of a piece of source code?

A. Steganography

B. Homomorphic encryption

C. Cipher suite

D. Blockchain

ANSWER: A

Explanation:

If you’re talking about hiding an audio file inside something that looks harmless—like source code—that points to **steganography**. Steganography is all about concealing data inside other data so it doesn’t look suspicious at first glance. Instead of encrypting the audio and making it obvious that “something secret” is there, it tries to make the audio blend in, like it’s just part of normal text or content.

The other choices don’t really fit. Homomorphic encryption is about doing math on encrypted data without decrypting it first, which is useful for privacy-preserving computing, not hiding files in code. A cipher suite is just a set of cryptographic algorithms used for secure connections (like TLS). Blockchain is a distributed ledger system, again unrelated to hiding an audio file inside source code.

So if you find weird-looking strings, unusual encoding, or chunks of data embedded in code that don't match the program's purpose, steganography is a strong clue.

References: https://www.britannica.com/technology/steganography and https://en.wikipedia.org/wiki/Steganography

QUESTION NO: 22

A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Choose two.)

A. Tokenization

B. Cryptographic downgrade

C. SSH tunneling

D. Segmentation

E. Patch installation

F. Data masking

ANSWER: C D

Explanation:

Since the legacy app can't be upgraded to use encryption, the next best move is to protect the traffic in transit some other way. **SSH tunneling** does exactly that: it wraps the old, cleartext protocol inside an encrypted SSH session, so anyone sniffing the network only sees encrypted packets. It's a classic "compensating control" when you're stuck with insecure protocols but still need to move data safely.

Segmentation is the other smart pick because it reduces exposure. By isolating that legacy system (and tightly controlling what it can talk to), you shrink the attack surface and limit who can intercept or tamper with the traffic. Even if the underlying protocol is weak, segmentation helps keep untrusted devices and users away from that network path.

Options like tokenization, masking, or patching don't really solve the "unencrypted in transit" problem here, and "cryptographic downgrade" is the opposite of what you want. References: https://www.ssh.com/academy/ssh/tunneling and https://www.cisa.gov/resources-tools/resources/implementing-network-segmentation

QUESTION NO: 23

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: C

Explanation:

Business email compromise (BEC) is when an attacker impersonates (or takes over) a trusted business account—often an executive, HR, or finance person—to trick staff into doing something risky, like sending money or handing over credentials. The key idea is social engineering using a "legitimate-looking" business identity and a high-trust request.

Option C fits that pattern well: an email that appears to be from the HR director asking for cloud admin credentials is a classic BEC-style move. Attackers love going after privileged accounts, and they often use authority ("HR director") to pressure the service desk into breaking process.

A is also suspicious, but it's more commonly described as basic phishing/spear phishing unless the scenario clearly indicates the executive's mailbox/domain was spoofed or compromised. B is ransomware delivered by attachment, and D is a standard credential-harvesting phishing link rather than the more targeted "internal business request" style typical of BEC.

References: https://www.ic3.gov/Media/Y2023/PSA230504 and https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

QUESTION NO: 24

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

Explanation:

The most direct, board-friendly consequence of data privacy non-compliance is **fines**. They're concrete, easy to understand, and you can usually point to a specific range or maximum penalty in the regulation. That makes them a clean way to justify spending: "If we don't fix this, we could owe $X."

Things like reputational damage and contractual issues are real, but they're harder to pin down. You can't always prove exactly how much revenue you'll lose, or how quickly it will happen. "Sanctions" can include different actions (like orders to stop processing data), but it's broader and less immediately measurable than a straight financial penalty.

So if the CISO needs a clear, immediate consequence to support a budget request, fines are the simplest and most persuasive option to put in front of the board. For reference, GDPR penalties are outlined here: https://gdpr-info.eu/issues/fines-penalties/ and California privacy penalty info can be found here: https://oag.ca.gov/privacy/penalties

QUESTION NO: 25

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: D E

Explanation:

To figure out which internal machine is “calling home” to a command-and-control (C2) server, you want the logs that show who talked to whom on the network. Network logs (like NetFlow, IDS/NSM, or packet capture summaries) are great for this because they typically record source IP, destination IP, ports, and timestamps. That makes it straightforward to spot internal IPs reaching out to the C2 infrastructure.

Firewall logs are the other big one. Even if the traffic was allowed, the firewall usually logs outbound connections and can show the internal source IP and the external destination (the C2). In many environments, firewall logs are the fastest way to confirm which host initiated the suspicious connection and whether it happened repeatedly.

DHCP logs can help later to map an IP address to a specific device/user, but they don’t directly prove C2 communication. App, auth, and database logs generally won’t be the best starting point for identifying the impacted host in a C2 scenario.

References: https://www.sans.org/white-papers/auditing-network-security/ and https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

QUESTION NO: 26

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

Explanation:

The biggest red flag here is the timing: the odd inbound/outbound traffic started right after the user installed sketchy software from a forum. That’s a classic setup for a backdoor—malware that quietly opens a way for someone on the internet to reach into the machine later.

The “uncommon port” detail matters because backdoors often use non-standard ports to blend in and avoid basic monitoring that focuses on common ports like 80, 443, or 3389. Once the backdoor is in place, it can call home to a command-and-control server, accept remote commands, and be used for things like data theft or dropping more malware.

A keylogger mainly focuses on capturing keystrokes; it might send data out, but the scenario is specifically about an unauthorized connection channel. Ransomware usually shows up as encrypted files and a ransom note, not just a weird port connection. “Fileless” describes how malware runs (in memory, using legit tools), but it doesn’t explain the purpose of the connection as directly as a backdoor does.

References: https://www.cisa.gov/news-events/news/understanding-backdoors-and-their-role-cyber-attacks and https://attack.mitre.org/techniques/T1133/

QUESTION NO: 27

A malicious insider from the marketing team alters records and transfers company funds to a personal account. Which of the following methods would be the best way to secure company records in the future?

A. Permission restrictions

B. Hashing

C. Input validation

D. Access control list

ANSWER: A

Explanation:

The core problem here is that someone who shouldn't have been able to change financial records had the access to do it. The best fix is to tighten who can read, write, or approve changes to those records using proper permission restrictions (think least privilege and separation of duties). Marketing users typically shouldn't have write access to finance systems, and sensitive actions like fund transfers should require higher privileges and ideally an approval workflow.

Hashing is great for detecting tampering (integrity checks), but it doesn't stop an authorized user from making "legitimate" changes if they already have access. Input validation mainly protects against bad or malicious input (like injection attacks), not insider privilege misuse. An ACL is a specific way to implement permissions, but the broader and best answer here is permission restrictions—locking down access so only the right roles can modify records.

References: https://csrc.nist.gov/glossary/term/least_privilege and https://www.nist.gov/privacy-framework/nist-privacy-framework-a-tool-improving-privacy-through-enterprise-risk-management

QUESTION NO: 28

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: A E

Explanation:

Because the issue is the web app's attack surface on port 443 (HTTPS), the best first move is to put something in front of the app that understands web traffic. That's exactly what a WAF does: it inspects HTTP/S requests and can block common web attacks like SQL injection and XSS before they ever hit the application. It's one of the most direct ways to reduce risk for an internet-facing web app.

Adding a NIDS is the other strong pick since you currently have no advanced network security monitoring. A NIDS watches network traffic for known bad patterns and suspicious behavior and alerts you when something looks like an attack. It won't "fix" the app, but it gives you visibility into scans, exploit attempts, and unusual traffic that could signal compromise.

The other options don't fit as well for this specific goal. A SIEM is great for log correlation, but it needs data sources like a WAF/NIDS to be truly useful. A HIPS focuses on the server itself (not the web traffic at the edge), and a CRL is about certificate validity, not attack reduction. A honeypot is more for research and deception than protecting the real app.

References: https://owasp.org/www-project-web-application-firewall/ and https://www.sans.org/white-papers/intrusion-detection-faq/

QUESTION NO: 29

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

Explanation:

A load balancer mainly helps with **availability**. The whole point is to keep an app or service reachable even when traffic spikes or when one server has problems. Instead of letting one system get overwhelmed (or become a single point of failure), the load balancer spreads requests across multiple healthy servers.

If a server goes down, most load balancers can stop sending traffic to it and route users to the remaining working servers. From the user's perspective, the service stays up, which is exactly what availability is about in the CIA triad.

The other choices don't fit as well. Confidentiality and privacy are more about preventing unauthorized access to data, and integrity is about preventing unauthorized changes. A load balancer can sometimes support those goals (like doing TLS termination), but its fundamental security win is keeping services online and resilient.

References: https://aws.amazon.com/elasticloadbalancing/ https://cloud.google.com/load-balancing/

QUESTION NO: 30

An organization's web servers host an online ordering system. The organization discovers that the servers are vulnerable to a malicious JavaScript injection, which could allow attackers to access customer payment information. Which of the following mitigation strategies would be most effective for preventing an attack on the organization's web servers? (Choose two.)

A. Regularly updating server software and patches

B. Implementing strong password policies

C. Encrypting sensitive data at rest and in transit

D. Utilizing a web-application firewall

E. Performing regular vulnerability scans

F. Removing payment information from the servers

ANSWER: A D

Explanation:

The two best picks here are keeping the web server and app stack patched (A) and putting a web application firewall in front of the site (D). If the JavaScript injection is tied to a known bug in the web app, framework, or a plugin, patching is what actually removes the weakness so the attack can't work in the first place.

A WAF helps from the "stop it at the door" side. It can detect and block common injection patterns (including XSS-style payloads) before they ever hit the application, which is especially useful when you can't patch immediately or you want an extra layer of defense.

The other options aren't as directly preventative for this specific issue. Strong passwords (B) help with account attacks, not script injection. Encryption (C) is great, but it doesn't stop the injection itself. Vulnerability scans (E) are important for finding issues, but they don't actively prevent exploitation. Removing payment info (F) reduces impact, but it's not a realistic "mitigation" for an ordering system and doesn't address the injection.

References: https://owasp.org/www-project-top-ten/ and https://owasp.org/www-project-web-application-firewall/

QUESTION NO: 31

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

Explanation:

Since the logins are coming from outside the organization and weren't done by real employees, this smells like stolen credentials being used remotely. The best way to cut down on that kind of attack is to make it harder for an attacker to successfully log in even if they have a password.

Conditional access policies help by putting rules around sign-ins, like blocking logins from unexpected countries, unknown devices, or risky IPs, and requiring extra checks when something looks suspicious. This directly targets the "outside the network" login problem. Microsoft's overview is a good example of how this works in real environments: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview.

Adding extra authentication factors (MFA) is the other big win. Even if an attacker has the username and password, they still need the second factor (app prompt, hardware token, etc.), which usually stops the takeover cold. NIST also backs MFA as a strong control for authentication security: https://pages.nist.gov/800-63-3/sp800-63b.html.

QUESTION NO: 32

Which of the following are common VoIP-associated vulnerabilities? (Choose two.)

A. SPIM

B. Vishing

C. Hopping

D. Phishing

E. Credential harvesting

F. Tailgating

ANSWER: A B

Explanation:

For VoIP systems, two classic problems you'll see come up are SPIM and vishing. **SPIM** is basically "spam over Internet messaging/telephony," where attackers blast unsolicited calls or messages through SIP/VoIP platforms. It's a VoIP-flavored nuisance, but it can also be used to push scams or malicious links.

Vishing (voice phishing) is also tightly tied to VoIP because it's cheap and easy for attackers to spoof caller ID and automate calling campaigns. The goal is to trick people into giving up sensitive info like account numbers, passwords, or MFA codes—just using phone calls instead of email.

The other choices can be security issues in general, but they aren't as specifically "VoIP-associated." For example, phishing and credential harvesting are broad attack categories, and tailgating is a physical security issue. "Hopping" isn't a standard VoIP vulnerability term in Security+ contexts.

References: https://www.fcc.gov/spoofing https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

QUESTION NO: 33

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

Explanation:

The fastest practical move for a newly found network-access flaw on old IoT gear is usually segmentation. Legacy IoT devices often can't be patched quickly (or at all), so you reduce risk by limiting what they can talk to and who can talk to them. Putting them in their own VLAN/subnet and locking it down with ACLs/firewall rules shrinks the attack surface and helps prevent an attacker from pivoting into the rest of your environment.

Patching would be great if a vendor fix exists and you can deploy it right away, but "legacy" devices are notorious for missing updates or breaking when updated. Replacement is the clean long-term answer, but it's rarely quick—procurement, testing, and rollout take time. Insurance doesn't mitigate the vulnerability; it only helps with financial impact after something goes wrong.

Good segmentation can be done quickly and gives immediate protection while you plan longer-term fixes like phased replacement. References: https://www.cisa.gov/news-events/news/understanding-network-segmentation and https://www.nist.gov/publications/guide-industrial-control-systems-ics-security (see network segmentation concepts).

QUESTION NO: 34

An organization wants to implement a secure solution for remote users. The users handle sensitive PHI on a regular basis and need to access an internally developed corporate application. Which of the following best meet the organization's security requirements? (Choose two.)

A. Local administrative password

B. Perimeter network

C. Jump server

D. WAF

E. MFA

F. VPN

ANSWER: E F

Explanation:

For remote users working with PHI, you want two big things: a protected connection back into the company network and strong proof that the person logging in is really the right user. A **VPN** gives you an encrypted tunnel over the internet, which helps prevent eavesdropping and keeps traffic to the internal app private while users are off-site.

MFA adds a second (or third) check beyond just a password, which is huge for protecting sensitive healthcare data. Even if a password gets phished or reused, MFA makes it much harder for an attacker to get in and reach that internal application.

The other options don't fit as well here: a jump server is more about controlled admin access, a WAF protects web apps from common attacks but doesn't solve secure remote connectivity by itself, and a perimeter network/DMZ is more for hosting public-facing services. For HIPAA-style risk reduction, VPN + MFA is the practical, standard combo. References: https://www.cisa.gov/resources-tools/resources/implementing-phishing-resistant-mfa and https://www.cloudflare.com/learning/access-management/what-is-a-vpn/

QUESTION NO: 35

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

Explanation:

The most secure choice here is a **bastion host** (also called a jump box). The idea is simple: instead of opening up multiple admin ports (like SSH/RDP) from the outside to lots of internal servers, you expose and harden one tightly controlled entry point. Admins connect to that one system first, and only then pivot to internal resources. That keeps the firewall rules narrow and reduces the overall attack surface.

A perimeter network (DMZ) is useful for hosting public-facing services, but it doesn't automatically solve the "admin access with minimal allowed traffic" problem by itself. A WAF mainly protects web apps (HTTP/HTTPS), not general administrative access to internal systems. Single sign-on helps with authentication and user experience, but it doesn't reduce the number of network paths/ports you'd otherwise have to allow through the boundary.

With a bastion host done right (MFA, strong logging, tight ACLs, patching, no direct internet browsing, and limited inbound rules), you get a clean choke point for monitoring and control—exactly what the question is aiming at.

References: https://en.wikipedia.org/wiki/Bastion_host and https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/bastion-hosts.html

QUESTION NO: 36

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

Explanation:

The best answer here is **jailbreaking**. Jailbreaking is when you remove or bypass the phone manufacturer's built-in restrictions (most commonly associated with Apple iOS). Once those limits are gone, you can install apps and tweaks that the official app store wouldn't normally allow, and you can unlock extra features the default OS doesn't provide.

Side loading is related, but it's not quite the same thing. Sideloading usually means installing an app from outside the official app store (like installing an APK on Android). That can be "unauthorized" in the sense that it didn't come from the store, but it doesn't necessarily unlock new OS-level features or remove the platform's restrictions the way jailbreaking does.

The other two options, **SQLi** and **cross-site scripting**, are web app attacks. They're about exploiting vulnerable websites or web apps, not about customizing a phone to add new features.

References: https://support.apple.com/guide/security/secure-boot-process-secac71d5623/web and https://en.wikipedia.org/wiki/Jailbreaking

QUESTION NO: 37

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

A. Configuring signature-based antivirus io update every 30 minutes

B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.

C. Implementing application execution in a sandbox for unknown software.

D. Fuzzing new files for vulnerabilities if they are not digitally signed

ANSWER: C

Explanation:

The big clue here is "custom malware." Brand-new, targeted malware often won't have a known signature yet, so simply updating signature-based antivirus frequently (A) still leaves a gap. You need something that can safely handle unknown or suspicious code.

Running unknown software in a sandbox (C) is the best fit because it isolates the program from the real system and lets you observe behavior (like file changes, network calls, or attempts to escalate privileges) without letting it harm endpoints. This helps whether the malware arrives via email attachment, a downloaded file, or a "parking lot USB" scenario—because the risky execution happens in a controlled environment.

S/MIME and USB encryption (B) are good security controls, but they don't stop a user from opening a malicious attachment, and encrypting a USB drive doesn't prevent malware from running. Fuzzing (D) is mainly for testing software for bugs during development, not for stopping malware that's already trying to execute on user machines.

For more background on sandboxing and malware analysis concepts, see https://www.cisa.gov/news-events/news/understanding-sandboxing and https://attack.mitre.org/techniques/T1496/ (MITRE ATT&CK techniques often observed during execution).

QUESTION NO: 38

A systems administrator is concerned about vulnerabilities within cloud computing instances. Which of the following is most important for the administrator to consider when architecting a cloud computing environment?

A. SQL injection

B. TOC/TOU

C. VM escape

D. Tokenization

E. Password spraying

ANSWER: C

Explanation:

The biggest cloud-specific worry in that list is **VM escape**. In a cloud environment, lots of customers' virtual machines sit on the same physical hardware, separated mainly by the hypervisor. If an attacker can "escape" from a guest VM into the hypervisor (or the host), they could potentially mess with other VMs on the same server. That's a much bigger architectural concern in cloud designs because it threatens the isolation that multi-tenant cloud security depends on.

The other choices are real security issues, but they're not as uniquely tied to cloud instance architecture. SQL injection is mostly an application-layer problem, password spraying is an identity/auth issue, and tokenization is a data protection technique (not a vulnerability). TOC/TOU is a race condition issue, but it's not the standout risk that specifically impacts the shared-hardware model the way VM escape does.

Good cloud architecture planning usually includes strong hypervisor hardening, patching, workload isolation, and monitoring for suspicious VM behavior—because if VM isolation fails, the blast radius can get ugly fast.

References: https://attack.mitre.org/techniques/T1611/ and https://nvd.nist.gov/

QUESTION NO: 39

Which of the following tools is best for logging and monitoring in a cloud environment?

A. IPS

B. FIM

C. NAC

D. SIEM

ANSWER: D

Explanation:

A SIEM (Security Information and Event Management) platform is the best fit here because its whole job is to collect logs from lots of different places, normalize them, and then help you monitor what's happening across your environment—including cloud services.

In the cloud, you typically have logs coming from workloads (VMs/containers), identity systems, cloud control planes, and network/security services. A SIEM pulls all of that into one place so you can search it, build dashboards, and set alerts for suspicious activity. That central visibility is what makes SIEM the go-to "logging and monitoring" answer on Security+.

The other options are useful, but they're not primarily cloud logging tools. IPS focuses on blocking/detecting malicious traffic, FIM watches for file changes on systems, and NAC controls who can connect to a network. None of those give you the broad, centralized log collection and correlation you get with SIEM.

References: https://www.nist.gov/publications/guide-computer-security-log-management and https://www.cisa.gov/resources-tools/services/security-information-and-event-management-siem

QUESTION NO: 40

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: C

Explanation:

The big issue here is that the phone is already stolen and the attacker successfully logged in. At that point, the fastest and most reliable way to protect company data is to erase it before it can be copied or abused. That's exactly what **remote wipe** is for—IT can send a command (usually through an MDM solution) to wipe the device and remove corporate data, even if the device isn't physically in the company's hands.

Full disk encryption is great, but it mainly helps when the attacker can't unlock the device. In this scenario, they logged in with valid credentials, so encryption won't stop them from accessing data while the phone is unlocked. **Containerization** and **application management** can reduce exposure by separating work data and controlling apps, but they don't solve the immediate "stolen and accessed" problem as cleanly as wiping the device.

Remote wipe is a standard mobile security control and is commonly implemented via MDM/EMM platforms. References: https://support.apple.com/guide/icloud/erase-a-device-mmfc0ef36f/icloud and https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-wipe

QUESTION NO: 41

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

Explanation:

This situation is a classic **tabletop exercise**. In a tabletop, the exec team (and other key players) sit together and talk through a realistic "what if" incident—like ransomware, a data breach, or a major outage—using the incident response plan as their guide. Nobody is actually pulling cables or taking systems offline; they're stress-testing the plan on paper and in conversation.

The value is in finding gaps before a real emergency hits: unclear decision-making, missing contact lists, confusion over who approves public statements, or delays in escalation. It's basically a safe, low-impact way to practice coordination and confirm everyone understands their role.

The other choices don't fit: continuity of operations is broader business continuity planning, capacity planning is about forecasting resource needs, and parallel processing is a computing concept—not an incident response test.

References: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf and https://www.cisa.gov/resources-tools/resources/tabletop-exercise-package

QUESTION NO: 42

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

Explanation:

For full-disk encryption (FDE), the big planning headache is always: “How do we unlock these drives safely, and how do we recover them when something goes wrong?” That’s why **key escrow** matters so much. If a user forgets their PIN, a laptop gets reassigned, or an employee leaves, you still need a controlled way to recover the encrypted data without resorting to shady workarounds or total data loss.

The other key item is **TPM presence**. A Trusted Platform Module can securely store encryption keys and support features like pre-boot integrity checks. In real deployments (like BitLocker), having a TPM often makes encryption easier to manage and harder for attackers to bypass by stealing keys off the drive. If some laptops don’t have TPMs (or have them disabled), you may need different policies (USB startup keys, PIN-only, or hardware refresh plans).

The other options (digital signatures, tokenization, CA linking, etc.) are useful in other security areas, but they’re not the core “make-or-break” planning concerns for rolling out FDE across laptops.

References: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-overview, https://www.nist.gov/publications/guidelines-media-sanitization

QUESTION NO: 43

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

A. Honey pot

B. Video surveillance

C. Zero Trust

D. Geofencing

ANSWER: A

Explanation:

A honeypot is made for exactly this situation: you set up a decoy system that looks real, then watch what attackers try to do to it. Since it’s not your real production server, you can safely collect logs, see tools and techniques, and learn what they’re after—without risking downtime or data loss on the actual environment.

The other choices don’t really fit the goal. Video surveillance is useful for physical security, but it won’t show you what an attacker is doing on your network. Zero Trust is a security model to reduce trust and tighten access, not a “trap” to observe attacker behavior. Geofencing can block or allow access based on location, but it doesn’t give you a controlled place to study attacks the way a honeypot does.

References: https://www.cisa.gov/news-events/news/understanding-honeypots and https://www.sans.org/blog/honeypots-101/

QUESTION NO: 44

A company plans to secure its systems by:

• Preventing users from sending sensitive data over corporate email

• Restricting access to potentially harmful websites

Which of the following features should the company set up? (Choose two.)

A. DLP software

B. DNS filtering

C. File integrity monitoring

D. Stateful firewall

E. Guardrails

F. Antivirus signatures

ANSWER: A B

Explanation:

To stop people from emailing out sensitive information, you'd set up DLP (Data Loss Prevention). DLP tools can scan email content and attachments for things like credit card numbers, SSNs, or internal documents, then block, quarantine, or warn the user before the message leaves the company. That's exactly what "preventing users from sending sensitive data over corporate email" is describing.

To limit access to risky or malicious sites, DNS filtering is a solid fit. It works by blocking or redirecting DNS lookups for known bad domains (phishing, malware, command-and-control, etc.), so users can't easily reach them even if they click a sketchy link. It's a simple, effective way to reduce web-based threats without relying only on the browser.

The other options don't match as well: file integrity monitoring watches for changes to files, a stateful firewall controls network sessions (not content leakage), "guardrails" is vague, and antivirus signatures mainly detect malware rather than preventing data exfiltration via email.

References: https://www.cisa.gov/resources-tools/resources/data-loss-prevention and https://www.cloudflare.com/learning/dns/what-is-dns-filtering/

QUESTION NO: 45

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

Explanation:

A buffer overflow is an application-layer bug, and in this case it was hit through a public website. The best “deployable” control in the list for protecting a web app from common exploit patterns is a WAF (Web Application Firewall). A WAF sits in front of the site and inspects HTTP/HTTPS traffic, looking for malicious payloads and behaviors (for example, suspicious inputs, abnormal request patterns, and known exploit signatures). It can block or rate-limit bad requests before they ever reach the vulnerable code.

An NGFW is great for network-level controls, but it’s not as tuned for web-app-specific attacks and doesn’t usually give the same depth of HTTP-aware protections as a WAF. TLS only encrypts traffic; it doesn’t stop an attacker from sending an exploit payload. SD-WAN is about routing and WAN optimization, not attack prevention.

In real life you’d still fix the root cause (patch the app, use safe coding practices, enable ASLR/DEP, and do testing), but for “what should you deploy” to reduce the chance of a repeat web exploit, WAF is the best fit.

References: https://owasp.org/www-community/Web_Application_Firewall and https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

QUESTION NO: 46

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

Explanation:

This is a **data retention** policy. The key clue is “archived for the proper time period.” Retention policies are all about how long you keep specific types of data (like transaction records) to meet legal, regulatory, or business requirements, and when it’s finally okay to delete or destroy it.

The other options don’t match that “keep it for X years” idea. A compromise is a security incident, analysis is about using the data, transfer is moving data around, and inventory is just figuring out what data you have and where it lives. None of those define how long records must be stored.

If you want a solid reference for how organizations should handle and protect sensitive data over its lifecycle (including keeping it only as long as needed), NIST has good guidance here: https://csrc.nist.gov/publications/detail/sp/800-122/final. For a practical view of retention schedules and why they exist, see: https://www.ibm.com/docs/en/filenet-p8-platform/5.5.x?topic=records-retention-schedules.

QUESTION NO: 47

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

Explanation:

The best picks here are **honeypots** and a **DNS sinkhole** because they help you spot bad activity *after* something is already inside your network.

A **honeypot** is basically a decoy system that looks interesting (and sometimes intentionally vulnerable). Legit users shouldn't be touching it, so if you see activity there, it's a strong signal an attacker is poking around. It's also useful for watching what they try to do next and collecting details about their behavior. Reference: https://www.cloudflare.com/learning/security/glossary/honeypot/

A **DNS sinkhole** helps catch compromised machines that are trying to "phone home" to command-and-control domains. When an infected host attempts to resolve a known malicious domain, the sinkhole redirects it somewhere you control, and the logs tell you which internal device made the request. That's a practical way to identify infected endpoints already on the network. Reference: https://www.infoblox.com/glossary/dns-sinkhole/

The other choices (tokenization, data obfuscation, CI/CD, threat modeling) are more about preventing issues or improving development/security planning, not actively detecting an intruder who's already in.

QUESTION NO: 48

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data? (Select TWO)

A. VPN

B. Drive encryption

C. Network firewall

D. File-level encryption

E. USB blocker

F. MFA

ANSWER: B E

Explanation:

Since the lab isn't connected to any outside networks, tools like a VPN or a network firewall don't really help with data loss. The biggest risk is usually someone walking data out on removable media or taking the storage device itself.

A USB blocker is a solid pick because it stops (or tightly controls) the most common "offline" exfil method: copying files to a thumb drive. If users can't plug in storage devices, it's much harder to quietly move data out of the lab.

Drive encryption is the other best choice because it protects data if a computer or hard drive is stolen, lost, or removed from the lab. Even if someone gets physical access to the disk, the contents should be unreadable without the key. For more background, see https://www.cisa.gov/resources-tools/resources/data-encryption and Microsoft's overview at https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ .

QUESTION NO: 49

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

Explanation:

Even though the switch stack adds redundancy inside the network, the internet edge is still hanging off a single ISP circuit. If that one ISP link goes down (provider outage, fiber cut, maintenance, regional issue), users lose external connectivity no matter how resilient the internal switching is.

That's the classic definition of a single point of failure: one component that can take down the whole service. To really improve availability end-to-end, you'd typically add a second ISP connection (ideally a different provider and physical path) and use failover routing.

The other choices don't fit as well. MTBF is about how often hardware tends to fail, but the main weakness here isn't the switch stack—it's the lone ISP. An SLA helps set expectations and penalties, but it doesn't remove the risk of outages. And RPO is a backup/recovery metric, not an availability issue for internet access.

References: https://en.wikipedia.org/wiki/Single_point_of_failure and https://aws.amazon.com/reliability/high-availability/

QUESTION NO: 50

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

Explanation:

The best choice is to modify the content of recurring training. These are existing users, and the goal is to help them adjust their day-to-day security mindset as they move back into a physical office. Updating recurring training lets you cover practical, office-specific risks like tailgating, shoulder surfing, badge use, clean desk expectations, secure printing, and what to do if they see an unknown person in a restricted area.

Periodic reminders (like quick emails) can help, but they usually don't go deep enough to build real situational awareness. Updating new-hire documentation misses the point because it targets people who aren't the main audience here. A phishing campaign is useful for testing and improving resistance to email-based attacks, but it doesn't directly address physical/environmental awareness in an office setting.

Refreshing recurring training content is the most complete way to align users with the current environment and reinforce the behaviors you actually need in the office. References: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-awareness-program and https://www.nist.gov/privacy-framework/nist-sp-800-50-building-information-technology-security-awareness-and-training-program

QUESTION NO: 51

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

A. Ease of recovery

B. Ability to patch

C. Physical isolation

D. Responsiveness

E. Attack surface

F. Extensible authentication

ANSWER: A E

Explanation:

When you're designing for high availability, you're really trying to keep services running even when something breaks. That's why **ease of recovery** matters so much. If a switch dies, a link drops, or a site goes down, you want clear failover paths, redundancy, and a recovery plan that gets you back to normal fast—without a bunch of manual work or long outages.

The other big piece is the **attack surface**. High availability doesn't mean much if attackers can easily knock your systems offline with a DDoS, exploit an exposed service, or move laterally because of weak segmentation. The more exposed and complex the network is, the more ways it can be disrupted. So HA design should include security controls that reduce exposure while still supporting uptime goals.

In short: build it so it can recover quickly, and secure it so it's harder to take down in the first place. References: https://www.nist.gov/cyberframework and https://www.cisa.gov/resources-tools/resources/denial-service-attacks

QUESTION NO: 52

Which of the following topics would most likely be included within an organization's SDLC?

A. Service-level agreements

B. Information security policy

C. Penetration testing methodology

D. Branch protection requirements

ANSWER: D

Explanation:

An organization's SDLC (software development life cycle) is all about how code is planned, built, reviewed, tested, and released. So the topics that fit best are the ones tied directly to software development and secure coding practices. "Branch protection requirements" is a great match because it's a common SDLC control in modern Git-based workflows—things like requiring pull requests, blocking direct pushes to main, enforcing code reviews, and requiring passing CI tests before a merge.

The other choices are important, but they don't really live inside the SDLC. Service-level agreements are more about vendor/service performance expectations. An information security policy is broader, high-level governance for the whole organization. And a penetration testing methodology is typically part of a security testing program and may happen around releases, but it's not usually a core "SDLC topic" the way secure repo controls are.

If you think of SDLC as "how we safely turn ideas into deployed code," branch protection is a day-to-day, built-in control that directly reduces risky changes and improves code quality.

References: https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/managing-protected-branches/about-protected-branches and https://owasp.org/www-project-samm/

QUESTION NO: 53

A Chief Information Security Officer is developing procedures to guide detective and corrective activities associated with common threats, including phishing, social engineering, and business email compromise. Which of the following documents would be most relevant to revise as part of this process?

A. SDLC

B. IRP

C. BCP

D. AUP

ANSWER: B

Explanation:

The document that best fits “detective and corrective activities” for threats like phishing and business email compromise is the Incident Response Plan (IRP). That’s the playbook teams use when something suspicious happens: how to spot it (detection), who to notify, how to contain it, how to eradicate it, and how to recover. If the CISO is writing procedures for dealing with these common attacks, the IRP is the place those step-by-step actions should live.

The other options don’t line up as well. SDLC is about building and maintaining software securely, not handling live security events. A BCP focuses on keeping the business running during major disruptions (like outages or disasters), not the detailed response steps for email-based attacks. An AUP tells users what they can and can’t do with company systems, which helps prevent issues, but it’s not the main document for detective/corrective response procedures.

For more detail on what an IRP covers and why it’s central to responding to incidents, see https://www.cisa.gov/resources-tools/resources/incident-response and https://www.nist.gov/privacy-framework/nist-sp-800-61.

QUESTION NO: 54

A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).

A. Private

B. Confidential

C. Public

D. Operational

E. Urgent

F. Restricted

ANSWER: B F

Explanation:

Because this is a government critical-system project, the fileshare data is almost certainly not meant for general internal use, and it definitely shouldn’t be shared widely. If details leaked (design docs, vulnerabilities, architecture, timelines), it could

create real-world risk—anything from mission failure to safety issues—so it needs a higher protection level than “Private” or “Public.”

That’s why **Confidential** fits: it’s sensitive information intended only for authorized people, and exposure could cause significant harm. In many classification schemes, “confidential” is the point where you start expecting tighter access controls, need-to-know, and stronger monitoring.

Restricted is also a good match because it implies the smallest audience and the highest impact if disclosed. For critical government work, it’s common to treat project info as restricted to a specific team, with strict permissions, logging, and often encryption.

The other choices don’t really describe data classification levels here. “Operational” and “Urgent” are more about context or priority, not sensitivity labels.

References: https://www.cisa.gov/topics/protecting-critical-infrastructure and https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

QUESTION NO: 55

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
Destruction
and

D. Classification

E. Sanitization

F. Enumeration

ANSWER: C E

Explanation:

When you’re reissuing a laptop, the main goal is to make sure none of the former employee’s data can be recovered by the next user. That’s why **sanitization** is a must. Sanitizing means securely wiping the drive (or using methods like crypto-erase) so the old files, cached data, saved passwords, and other leftovers aren’t sitting there waiting to be recovered with simple tools.

Destruction is also a valid data-handling activity, but it’s usually used when the device (or at least the storage media) is being disposed of, not reissued. Still, since the question asks for the “best combination” of data handling activities and includes destruction as an option, the intended pairing is **sanitization + destruction** to guarantee the data is unrecoverable (especially for highly sensitive data or strict compliance cases).

For a solid standard reference on how sanitization and destruction fit into media handling, see NIST SP 800-88 Rev. 1: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

QUESTION NO: 56

A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?

• The solution must be inline in the network

• The solution must be able to block known malicious traffic

• The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS

B. NIDS

C. HIPS

D. NIPS

ANSWER: D

Explanation:

The key phrase here is *inline in the network*. An inline security tool can actually sit in the traffic path and take action on packets as they pass through. That rules out IDS options (like NIDS), because IDS is mainly for detecting and alerting, not actively blocking.

A **Network Intrusion Prevention System (NIPS)** is built for exactly what the requirements describe: it runs inline, inspects network traffic, and can automatically block or drop traffic that matches known bad signatures or suspicious patterns. That also makes it a strong fit for stopping network-based attacks like scans, exploit attempts, and certain denial-of-service patterns.

HIDS/HIPS focus on protecting individual hosts (servers/endpoints) rather than monitoring and stopping threats across the network. Since the goal is to block malicious traffic and stop attacks at the network level, NIPS is the best match.

References: https://www.cisco.com/c/en/us/products/security/intrusion-prevention-system-ips/index.html and https://www.fortinet.com/resources/cyberglossary/intrusion-prevention-system

QUESTION NO: 57

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

Explanation:

Tagging laptops and tying them to employee IDs mainly improves accountability. If something bad happens—like malware, data exfiltration, or a policy violation—you can quickly figure out who had that exact device and reach the right person fast. That saves a lot of time during triage and incident response because you're not guessing who used which laptop.

It also helps a ton during offboarding. When someone leaves, asset records make it clear what equipment (and therefore what company data) they were responsible for. That makes it easier to recover the laptop, confirm it's returned, and take the right steps like wiping it or locking it down if it goes missing. In other words, it reduces the chance that company data walks out the door unnoticed.

These are classic asset management wins: better tracking, clearer ownership, and faster response when something goes wrong. For more on why inventory and asset tracking matter, see https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final and https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

QUESTION NO: 58

Due to a cyberattack, a company's IT systems were not operational for an extended period of time. The company wants to measure how quickly the systems must be restored in order to minimize business disruption. Which of the following would the company most likely use?

A. Recovery point objective

B. Risk appetite

C. Risk tolerance

D. Recovery time objective

E. Mean time between failure

ANSWER: D

Explanation:

The metric that answers “how fast do we need to be back up?” is the **Recovery Time Objective (RTO)**. RTO is the target maximum downtime for a system or process after an outage (like a cyberattack). If the business says, “email must be restored within 4 hours” or “the payment system must be back within 30 minutes,” those are RTOs.

The other options don’t quite fit. **RPO** is about how much data loss is acceptable (how far back you can roll to a backup), not how quickly you restore service. **Risk appetite** and **risk tolerance** describe how much risk the business is willing to accept, but they don’t directly measure recovery speed. **MTBF** is a reliability metric (average time between failures), which is useful for hardware planning but doesn’t set a recovery deadline after an incident.

References: https://www.nist.gov/privacy-framework/nist-privacy-framework-glossary#rto and https://www.cloudflare.com/learning/security/glossary/rto-recovery-time-objective/

QUESTION NO: 59

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

Explanation:

This is a classic smishing (SMS phishing) scam: it uses urgency ("I'm in an airport"), authority (pretending to be the CEO), and an unusual payment method (gift cards) to push people into acting fast without verifying.

The best immediate response is to warn everyone right away. Sending a general company email helps stop the bleeding by telling employees not to buy anything, not to reply, and to report similar texts. That's quick, practical damage control.

The other strong response is to turn it into a training moment. Adding a smishing exercise to annual security awareness training helps employees recognize these red flags next time—especially the "CEO needs gift cards" pattern, which is extremely common in real-world scams.

The other choices don't fit as well. Canceling legitimate gift cards doesn't address the scam. Making the CEO change numbers or forensically investigating the CEO's phone assumes the CEO was compromised, which isn't indicated here (the attacker can spoof identity). MDM can be helpful overall, but it's not the best targeted response to this specific social engineering incident.

References: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks and https://www.ftc.gov/business-guidance/blog/2018/08/scammers-demand-gift-cards

QUESTION NO: 60

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

Explanation:

Since the company already rolled out single sign-on (SSO), the new cloud accounting app should be hooked into that same SSO setup so users can log in with their existing company identity. In most enterprise "SSO to a cloud app" deployments, that integration is done with SAML, where the company's identity provider (IdP) sends a signed authentication assertion to the software vendor (the service provider).

RADIUS and EAP are more about network access (like Wi-Fi/VPN authentication) than logging into SaaS business apps. OpenID (often meaning OpenID Connect) can also do SSO, but in many corporate SaaS integrations—especially the classic "enterprise SSO" story—SAML is the most common and is exactly what you'd configure when onboarding a new third-party cloud application into an existing SSO environment.

References: https://www.okta.com/identity-101/what-is-saml/ and https://learn.microsoft.com/en-us/entra/identity-platform/saml-protocol-reference

QUESTION NO: 61

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

Explanation:

Putting an end-of-life server into a tightly restricted VLAN is a classic **technical** control. VLANs, ACLs, and routing rules are all technology-based settings that limit who can talk to what on the network. In other words, the team is using network configuration to enforce access restrictions.

It's also a **compensating** control. Since the server is end-of-life, it likely can't be properly patched or upgraded, so the team reduces risk in another way by isolating it and only allowing access from specific devices. That doesn't "fix" the underlying problem (unsupported software), but it helps compensate for it by shrinking the attack surface.

Detective controls would be things like logging/monitoring, and corrective controls would be actions that remediate after an issue. Here, the focus is preventing exposure through segmentation, so technical + compensating fits best.

References: https://www.cisa.gov/resources-tools/resources/defense-depth and https://www.nist.gov/privacy-framework/nist-privacy-framework-control-catalog

QUESTION NO: 62

A company installed cameras and added signs to alert visitors that they are being recorded. Which of the following controls did the company implement? (Choose two.)

A. Directive

B. Deterrent

C. Preventive

D. Detective

E. Corrective

F. Technical

ANSWER: B D

Explanation:

The best matches here are **Deterrent** and **Detective**.

The cameras plus the "you are being recorded" signs are a classic **deterrent control** because they're meant to discourage bad behavior before it happens. A lot of people won't try something shady if they know they'll be on video, so the control is influencing behavior just by being visible. (See: https://www.sans.org/information-security-glossary/deterrent-control/)

At the same time, cameras are also a **detective control** because they record what's going on so you can review footage after an incident. That helps you spot what happened, when it happened, and who was involved—basically evidence gathering and incident confirmation. (See: https://csrc.nist.gov/glossary/term/detective_control)

The other choices don't fit as well: it's not really **directive** (that's more policies/rules), not **preventive** (it doesn't physically stop the act), and not **corrective** (it doesn't fix anything after the fact). Cameras are "technical" in a general sense, but the question is clearly asking for the control *type/purpose*, which is deterrent and detective.

QUESTION NO: 63

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

ANSWER: A

Explanation:

The best match here is GDPR. It's a privacy law that's specifically built around people's rights over their personal data. That's why you'll see clear wording in GDPR about things like being told what data is collected (right to be informed), being able to request a copy of your data (right of access), and asking for your data to be erased in certain cases (right to be forgotten/right to erasure).

PCI DSS doesn't really fit because it's a security standard focused on protecting payment card data for businesses that handle card transactions. NIST is also not about individual privacy rights—it's a set of cybersecurity frameworks and guidelines organizations can choose to follow, but it doesn't create legal rights like "erase my data."

If you want to double-check the exact rights listed, GDPR's text and summaries are easy to find here: https://gdpr-info.eu/ and the UK ICO's GDPR guide is also very practical: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

QUESTION NO: 64

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

Explanation:

The best fit here is a **cold site** because it's the cheapest disaster recovery option to maintain. A cold site is basically an empty (or mostly empty) facility with the basics like space, power, and cooling, but without fully installed servers and real-time data replication. That keeps monthly costs low, which matches management's "keep it to a minimum" requirement.

The question also says there's no budget for extra internet connections. Hot sites and many warm-site setups usually depend on stronger connectivity and ongoing synchronization to be truly "ready to go," which adds cost. With a cold site, you accept a longer recovery time (you'll be bringing in equipment and restoring from backups), but you avoid paying for duplicate, always-on infrastructure and extra network links.

"Failover site" isn't really a standard site type like hot/warm/cold—it describes the action/process of switching over, not a specific cost-controlled facility choice.

References: https://www.ready.gov/business/implementation/it and https://www.cisa.gov/resources-tools/resources/disaster-recovery-plan

QUESTION NO: 65

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

Explanation:

This is a classic smishing (SMS phishing) + CEO impersonation scam. The fastest, most practical move is to warn everyone right away so the message stops spreading and nobody buys gift cards “just to be safe.” A company-wide email (or Teams/Slack alert) helps employees recognize the scam, report it, and ignore any follow-up texts.

The second best response is to build this exact scenario into security awareness training. Smishing works because it feels urgent and personal, and people don’t stop to verify. A short training exercise teaches staff to slow down, confirm requests using a trusted channel, and watch for common red flags like gift cards, urgency, and off-policy payment methods.

Things like changing the CEO’s number or doing phone forensics don’t really fix the core issue, because the attacker likely spoofed the number and never touched the CEO’s device. Mobile device management can help overall, but it’s not the best immediate response to this specific incident.

References: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks and https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

QUESTION NO: 66

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

Explanation:

The password rules (10 characters, letters, numbers, and special characters) are a classic example of **password complexity**. That's the company setting a policy to make passwords harder to guess or brute-force, which directly helps protect intranet accounts.

The second part—using the intranet profile to give access to other company-owned websites—points to **federation**. With federation, one trusted identity (the intranet account/IdP) can be used to access multiple related services (service providers) without creating separate logins everywhere. It's essentially using the intranet identity to "carry" permissions across sites.

Options like identity proofing are more about verifying who the person is during enrollment, and OAuth is mainly about delegated authorization (often third-party app access), not the general "one company login for many internal sites" idea described here.

References: https://www.cisa.gov/resources-tools/resources/implementing-strong-authentication and https://www.okta.com/identity-101/what-is-federation/

QUESTION NO: 67

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? (Select two).

A. Key escrow

B. TPM presence

C. Digital signatures

D. Data tokenization

E. Public key management

F. Certificate authority linking

ANSWER: A B

Explanation:

For full-disk encryption (FDE), two planning items matter a lot more than the rest: how you'll recover data if something goes wrong, and what hardware will securely protect the keys. That's why **key escrow** is a big deal. If a user forgets their PIN, a laptop's motherboard dies, or a device gets reassigned, you still need a safe, controlled way to recover the encryption keys and get business data back.

TPM presence is the other key factor. A TPM can securely generate and store encryption key material and help tie the drive's encryption to the device's trusted boot state. In real life, this usually makes FDE stronger and smoother to manage (for example with BitLocker using TPM-backed protectors), and it reduces the risk of keys being stolen from software storage.

The other choices (digital signatures, tokenization, PKI/CA linking) are useful in other security projects, but they're not the core planning concerns for rolling out laptop FDE across an org.

References: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-overview and https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

QUESTION NO: 68

A university employee logged on to the academic server and attempted to guess the system administrators' log-in credentials. Which of the following security measures should the university have implemented to detect the employee's attempts to gain access to the administrators' accounts?

A. Two-factor authentication

B. Firewall

C. Intrusion prevention system

D. User activity logs

ANSWER: D

Explanation:

D. User activity logs are the best fit because they directly record what the employee is doing on the server, including repeated failed login attempts against admin accounts. If someone is trying to guess passwords, the evidence shows up as a pattern in the logs (lots of failures, specific usernames targeted, timestamps, source workstation/IP, etc.). That's exactly what you need for detection and investigation.

Two-factor authentication helps *stop* an attacker from successfully logging in, but it doesn't automatically "catch" or report the guessing behavior by itself. A firewall mainly watches and filters network traffic, and it's not designed to track detailed user login behavior on a server. An IPS can sometimes spot brute-force attempts on the network, but it's not as reliable for OS/application-level login auditing as the server's own authentication and activity logs.

If the university also forwards those logs into a SIEM, they can alert in real time when there are too many failed logins or suspicious access attempts. For more on log management, see NIST SP 800-92:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

QUESTION NO: 69

Which of the following are the best security controls for controlling on-premises access? (Choose two.)

A. Swipe card

B. Picture ID

C. Phone authentication application

D. Biometric scanner

E. Camera

F. Memorable question

ANSWER: A D

Explanation:

For controlling access to an on-premises building or secure room, you usually want controls that actually restrict entry at the door. A swipe card (badge) is a classic physical access control because it ties entry to a specific credential and can be logged, disabled quickly, and limited by time or location.

A biometric scanner is another strong choice because it verifies something you are (like a fingerprint or iris). That makes it much harder for someone to "borrow" access the way they could with a badge alone, especially when combined with a card reader for two-factor physical access.

Options like cameras and picture IDs can help with monitoring and verification, but they don't reliably prevent entry by themselves. Phone authentication apps and memorable questions are mainly for logical (system) access, not doors. For more on physical access controls, see https://www.cisa.gov/resources-tools/resources/physical-security and https://www.nist.gov/publications/access-control-systems.

QUESTION NO: 70

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: B E

Explanation:

When you're reissuing a laptop, the big goal is to make sure none of the former employee's data can be recovered and that the device is safe to hand to someone else. That's where **sanitization** comes in—it's the practical step of wiping or securely erasing storage so old files, cached credentials, and sensitive data aren't left behind.

The other good fit here is **certification**. After sanitizing, you typically want proof that the wipe was done correctly (often required by policy, audits, or compliance). Certification is basically documenting/attesting that the sanitization met the required standard, which helps protect the company if questions come up later.

Options like retention, classification, and enumeration don't really address reissuing a device. And while **destruction** is a valid data handling method, it's usually used when you're disposing of media—not reusing the laptop.

References: https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final and https://www.iso.org/standard/45306.html

QUESTION NO: 71

A security analyst needs to improve the company's authentication policy following a password audit. Which of the following should be included in the policy? (Choose two.)

A. Length

B. Complexity

C. Least privilege

D. Something you have

E. Security keys

F. Biometrics

ANSWER: A B

Explanation:

Since this was a *password* audit, the policy updates should focus on what makes passwords harder to guess or crack. The two big basics are password **length** and **complexity**. Longer passwords are dramatically harder to brute-force, and they also tend to be more resistant to common wordlist attacks.

Complexity (using a mix of character types, avoiding common patterns, and not reusing easy variations) helps reduce the chance that users pick something predictable. That said, modern guidance often prioritizes length over "weird character rules," but complexity is still a common policy requirement in many organizations and exam objectives.

Options like **least privilege** are important, but they're about authorization, not password rules. The other choices (something you have, security keys, biometrics) are authentication factors for MFA/passwordless sign-in. They can strengthen authentication overall, but they aren't password-policy items you'd typically add specifically because of a password audit.

References: https://pages.nist.gov/800-63-3/sp800-63b.html and https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords

QUESTION NO: 72

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: B

Explanation:

Correct answer: B. Chain of custody

When you're dealing with an incident, it's not enough to just grab logs, disk images, or other artifacts—you also have to prove they weren't tampered with. That's exactly what *chain of custody* is for. It's the step-by-step record showing who collected the evidence, when they collected it, where it was stored, who accessed it later, and what (if anything) was done to it. If that paper trail is missing or sloppy, the evidence can be questioned or thrown out during legal action or even an internal disciplinary process.

The other choices are related, but they don't cover the "handled properly end-to-end" part. *Legal hold* stops deletion, *preservation* focuses on keeping data intact, and *e-discovery* is about finding and producing electronic info for legal matters. Only chain of custody directly tracks every handoff and protects the integrity of the evidence lifecycle.

References: https://csrc.nist.gov/pubs/sp/800/86/final and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION NO: 73

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

A. Upgrade the bandwidth available into the datacenter

B. Implement a hot-site failover location

C. Switch to a complete SaaS offering to customers

D. Implement a challenge response test on all end-user queries

ANSWER: D

Explanation:

A long-running DDoS that chews up database resources is mostly an availability problem, so the best move is to stop junk traffic before it can hit the app and force expensive database work. A challenge-response check (like CAPTCHAs, JavaScript challenges, or other bot-detection steps) helps separate real users from automated floods, which reduces the number of requests that make it through to the database.

Just “buying more bandwidth” can help with simple volumetric attacks, but it doesn’t fix the core issue here—requests that still reach the application and trigger heavy database queries. A hot site is great for disaster recovery, but it’s expensive and doesn’t automatically prevent the same DDoS pattern from taking down the failover site too unless you also add DDoS controls. Moving everything to SaaS is a huge business change and not the most likely quick recommendation for this specific scenario.

So, adding challenge-response at the edge is a practical mitigation that directly targets the attack behavior and protects the database from being overwhelmed. References: https://www.cloudflare.com/learning/bots/how-captchas-work/ and https://www.cloudflare.com/learning/ddos/ddos-attack/

QUESTION NO: 74

A company plans to secure its systems by:

• Preventing users from sending sensitive data over corporate email

• Restricting access to potentially harmful websites

Which of the following features should the company set up? (Choose two.)

A. DLP software

B. DNS filtering

C. File integrity monitoring

D. Stateful firewall

E. Guardrails

F. Antivirus signatures

ANSWER: A B

Explanation:

To stop employees from sending sensitive info out through corporate email, the best fit is Data Loss Prevention (DLP). DLP tools can scan email content and attachments for things like credit card numbers, SSNs, customer records, or specific keywords, then block, quarantine, or encrypt messages based on policy. That directly matches the “prevent users from sending sensitive data” requirement.

To restrict access to risky or known-bad websites, DNS filtering is a solid choice. It blocks or redirects requests to malicious domains (phishing, malware, command-and-control, etc.) before the connection even happens, which is a simple way to reduce drive-by infections and credential theft across the whole network.

The other options don’t line up as well: file integrity monitoring is about detecting unauthorized file changes, a stateful firewall focuses on network connections (not categorizing websites), “guardrails” is vague, and antivirus signatures don’t control where users browse or prevent data from being emailed out.

References: https://www.cisa.gov/news-events/news/understanding-data-loss-prevention-dlp and https://www.cisa.gov/news-events/news/using-dns-protective-services

QUESTION NO: 75

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

Explanation:

This is a classic smishing (SMS phishing) / impersonation scam. The quickest, most practical response is to warn people right away so nobody follows the instructions and buys gift cards. That's why sending a general company-wide warning email is a top choice—it helps stop the damage fast and reminds everyone to verify unusual requests through a trusted method.

The second best response is to turn it into targeted awareness training by adding a smishing exercise. These scams work because they feel urgent ("airport," "no email") and use authority ("CEO") to pressure employees. A realistic smishing drill and refresher training teaches staff to slow down, verify out-of-band, and report messages instead of acting on them.

The other options don't fit as well. Canceling gift cards doesn't address the scam, changing the CEO's number is a knee-jerk reaction, and forensics on the CEO's phone assumes the CEO was compromised (this could just be spoofing). MDM is useful overall, but it's not the best immediate response to this specific social engineering incident.

References: https://www.cisa.gov/topics/cyber-threats-and-advisories/phishing, https://www.ftc.gov/business-guidance/blog/2018/08/scammers-use-gift-cards-their-favorite-way-steal-money

QUESTION NO: 76

A security engineer is building a file transfer solution to send files to a business partner over the internet, and it needs to be secure. Users will drop files into a specific directory and the server will send them to the partner. Which of the following can be used?

A. S/MIME

B. LDAPS

C. SSH

D. SRTP

E. SFTP (SSH File Transfer Protocol)

ANSWER: C E

Explanation:

The best fit here is **SSH**, because it's the common secure "tunnel" used for file transfers over the internet. In real deployments, this usually means using **SFTP** (SSH File Transfer Protocol) or **SCP**, both of which run over SSH and encrypt the session end-to-end. That gives you confidentiality and integrity while the server pushes files to the partner.

The other options don't really match a secure file transfer workflow. **S/MIME** is for encrypting and signing email messages, not moving files between servers. **LDAPS** is LDAP directory access over TLS (good for authentication/directory queries), not file transfer. **SRTP** is for securing real-time voice/video streams, like VoIP.

So if you're setting up a "drop folder" and then sending files out securely across the internet, SSH (typically via SFTP) is the practical, correct choice.

References: https://www.rfc-editor.org/rfc/rfc4251 and https://www.openssh.com/

QUESTION NO: 77

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

Explanation:

This is a classic case of **smishing** plus **impersonation**. Because the message arrives as a text/SMS, it falls under smishing (SMS-based phishing). The attacker is using the text to push the employee into “verifying” credentials, which is really just a way to steal login details.

At the same time, the sender is pretending to be the payroll department, which is **impersonation**. The whole trick works because people tend to trust internal departments—especially payroll—so they’re more likely to respond quickly without double-checking.

It’s not vishing because there’s no voice call involved, and typosquatting would be more about a lookalike domain name or URL. “Phishing” is the broader umbrella term, but since the question is asking for two techniques and one is clearly SMS-based, **smishing** is the best, most specific fit along with impersonation.

References: https://www.cisa.gov/resources-tools/resources/avoiding-social-engineering-and-phishing-attacks and https://www.fcc.gov/scams

QUESTION NO: 78

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

Explanation:

“Most impacted when it is lost” is really pointing at the availability side of the CIA triad. If the business can’t function without the data (or can’t meet safety, legal, or operational requirements), then losing it causes the biggest immediate damage. That’s what “critical” data means: it’s essential for operations, and downtime or permanent loss has a major impact.

“Confidential” and “private” focus more on what happens if the data is exposed to the wrong people (confidentiality). That’s definitely serious, but it’s a different kind of harm than “we can’t operate because the data is gone.” “Public” data is meant to be shared anyway, so losing it is usually the least damaging.

This idea lines up with standard security thinking around CIA: availability is about keeping systems and data accessible when needed, and critical data is the stuff you protect most heavily against loss (backups, redundancy, DR plans, etc.).

References: https://www.nist.gov/cyberframework, https://www.cisa.gov/resources-tools/resources/cia-triad

QUESTION NO: 79

Which of the following would enable a data center to remain operational through a multiday power outage?

A. Generator

B. Uninterruptible power supply

C. Replication

D. Parallel processing

ANSWER: A

Explanation:

A generator is the practical answer for staying online during a multiday outage. Once utility power drops, an on-site generator can keep supplying electricity as long as there's fuel (and it's maintained and tested). That's exactly what data centers rely on for long-duration power loss.

An uninterruptible power supply (UPS) is still important, but it's mainly there to cover the short gap between losing utility power and the generator kicking in, or to allow a clean shutdown. Most UPS systems only last minutes to maybe an hour or two, not multiple days.

Replication can help with availability if you fail over to another site, but it doesn't keep the same data center operational during the outage. Parallel processing is about performance, not power resilience.

References: https://www.cisa.gov/resources-tools/resources/maintaining-business-continuity-during-power-outages and https://en.wikipedia.org/wiki/Emergency_power_system

QUESTION NO: 80

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: D

Explanation:

Since the design is already released, the "next best practice" step isn't to redesign it informally—it's to route the findings through the official change control process. Change control makes sure proposed fixes are documented, reviewed, risk-assessed, tested, approved, and scheduled in a controlled way, instead of someone quietly tweaking production designs.

A risk management process is definitely involved, but it's usually part of evaluating the change request, not the main "next step" after issues are found. A product design process would apply if you were still creating the initial design, and a design review process is what you just did—this annual review is essentially a design review that surfaced the issues.

In short: once issues are identified in a live/released system, you open a change request and follow change control so you keep traceability and avoid breaking things unexpectedly. References: https://en.wikipedia.org/wiki/Change_control and https://www.itil.org/ (ITIL change enablement/change control concepts).

QUESTION NO: 81

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: B

Explanation:

The best answer is **B. Request process for data subject access**. In real-world privacy programs, one of the fastest ways to get in trouble is not being able to handle people's privacy requests correctly and on time. Most privacy laws (like GDPR and CCPA) give individuals clear rights to access, delete, or get a copy of their personal data, and organizations need a repeatable process to make that happen.

A solid DSAR (data subject access request) process also forces you to solve the hard parts of privacy: verifying identity, finding data across systems, filtering out info that belongs to other people, and responding within legal deadlines. If you can't do those things, your "privacy program" is mostly just paperwork.

The other choices matter, but they're not as directly tied to day-to-day compliance. Reporting structure (A) helps governance, controller vs. processor (C) affects responsibilities, and location (D) influences which laws apply—but none of those matter much if you can't actually fulfill user rights requests.

References: https://gdpr-info.eu/art-15-gdpr/ and https://oag.ca.gov/privacy/ccpa

QUESTION NO: 82

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

Explanation:

For a high-availability network, you're mainly trying to keep services up even when something breaks. That's why **ease of recovery** matters so much: if a router, link, or firewall fails, you want quick failover, simple restore steps, and minimal manual work so downtime stays tiny.

Responsiveness is the other big one. High availability isn't just "it's online"—it's also about the network reacting fast to problems and load changes. Things like routing convergence, health checks, load balancing, and monitoring/alerting all play into how quickly the network can detect trouble and shift traffic to healthy paths.

The other choices are more security- or operations-focused. Patching is important, but it's not a core HA design requirement. Physical isolation and attack surface reduction help security, not uptime. Extensible authentication is useful for access control, but it doesn't directly keep the network running during failures.

References: https://learn.microsoft.com/en-us/azure/architecture/framework/resiliency/design and https://wa.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html

QUESTION NO: 83

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

Explanation:

The best reasons to decommission a network device are the ones you can't realistically "fix" with a config change. If the device can't meet your organization's encryption requirements, that's a big red flag. It usually means the hardware/firmware is too old to support modern crypto (for example, strong TLS versions or approved ciphers). At that point, keeping it around forces you to accept weaker protection for data in transit, which is exactly how older gear becomes the weak link attackers look for.

Likewise, if the device can't receive authorized updates (vendor support ended, no signed firmware available, or patching is no longer possible), it becomes a permanent risk. New vulnerabilities will keep showing up, and without patches you're basically stuck running known-bad software on your network. Segmentation can reduce exposure, but it doesn't remove the underlying problem—an unpatchable device is still untrustworthy.

For reference, NIST emphasizes strong cryptography and timely patching as core security controls: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final and guidance on patch management: https://www.cisa.gov/resources-tools/resources/understanding-patch-management.

QUESTION NO: 84

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

Explanation:

For basic server hardening, you want to reduce easy ways in and shrink the attack surface before the box ever goes live. Disabling default accounts is a big one because attackers love predictable usernames (like “admin” or “guest”) and will try common defaults first. If those accounts aren’t needed, turning them off removes a very common entry point. CIS calls this out as part of secure configuration and account management practices: https://www.cisecurity.org/controls/account-management

Removing unnecessary services is the other classic hardening step. Every extra service is another listening port, another codebase to patch, and another potential vulnerability. If the server doesn’t need a service, uninstalling or disabling it cuts down what an attacker can probe or exploit. This aligns with the idea of minimizing exposed functionality, which NIST discusses in secure configuration guidance: https://csrc.nist.gov/publications/detail/sp/800-123/final

The other choices aren’t “wrong” in general, they’re just not the best answers for hardening specifically. Asset inventory is governance, SIEM forwarding is monitoring, joining a domain is management, and documenting default passwords is actually risky unless you’re documenting that they were changed and stored securely.

QUESTION NO: 85 - (HOTSPOT)

HOTSPOT

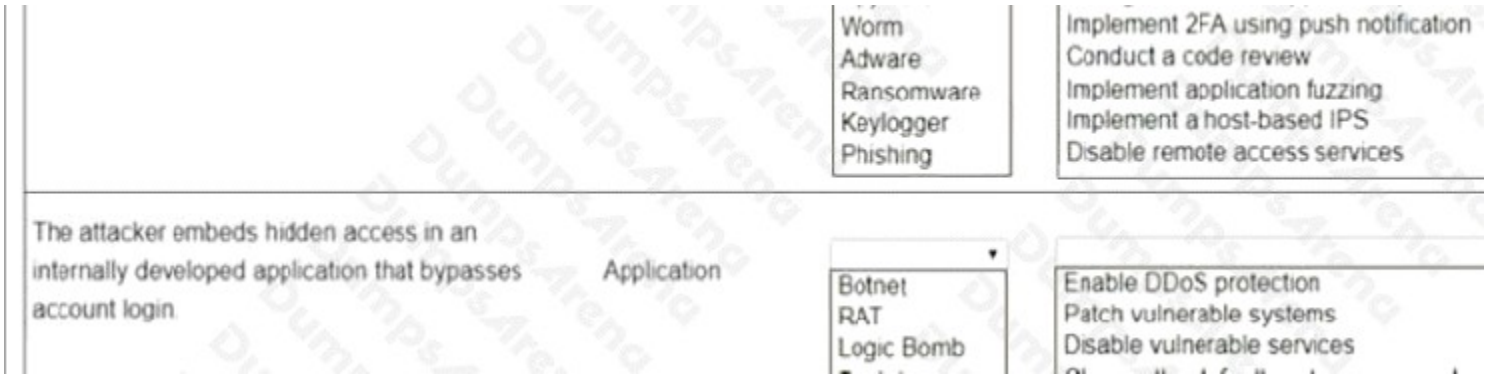
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

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
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 passwo 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 passwo 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 passwo 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	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application passwo Implement 2FA using push notification Conduct a code review Implement application fuzzing



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Act
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	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

ANSWER:

Explanation:

Web server Botnet Enable DDoS protection

User RAT Implement a host-based IPS

Database server Worm Change the default application password

Executive Keylogger Disable vulnerable services

Application Backdoor Implement 2FA using push notification

QUESTION NO: 86

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

Explanation:

For insider data exfiltration, removable media is one of the most common and straightforward paths. If someone already has access to sensitive files, copying them to a USB drive (or other removable storage) is fast, easy to hide, and doesn't require fancy hacking. That's why "unidentified removable devices" is the best fit here—plug it in, copy data out, walk away.

The other options are more typical of external attackers. Default network device credentials are about breaking into infrastructure, spear phishing is usually used to trick users into giving access, and typosquatting is a branding/domain trick to fool people into visiting a fake site. An insider already has a foothold, so they often don't need those tactics to get data out.

Real-world guidance also calls out removable media as a classic exfiltration method and a common insider risk, which is why many orgs restrict USB use or require device control tools. References: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final and https://www.cisa.gov/insider-threat-mitigation

QUESTION NO: 87

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: C D

Explanation:

Correct answers: C (Signage) and D (Sensor).

Signage is a simple but effective control because it works on people's behavior. A clear "Authorized Personnel Only" or "Area Under Video Surveillance" sign can make someone think twice before trying anything, so it's a deterrent. It also supports detection in a practical way: if someone goes past a posted warning, it's easier to treat that as suspicious/unauthorized activity and respond appropriately.

Sensors (like door contacts, motion detectors, and alarm sensors) are built for detection—they trigger an alert when something happens. They also deter when they're visible or when people know alarms are in place, since the risk of getting caught goes way up. That mix of "I'll be noticed" and "I'll be stopped quickly" is exactly what you want for both detection and deterrence.

Lighting, fencing, bollards, and locks are great physical protections, but by themselves they lean more toward prevention/delay. They don't reliably "notice and report" an event unless paired with monitoring or alarm tech.

References: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final and https://www.cisa.gov/resources-tools/resources/physical-security

QUESTION NO: 88

A company wants to simplify the certi cate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet. Which of the following BEST describes the type of certi cate the company should implement?

A. Subject alternative name

B. Wildcard

C. Self-signed

D. Domain validation

ANSWER: B

Explanation:

A wildcard certificate is the cleanest way to manage "one domain, lots of subdomains." With a wildcard (for example, `*.example.com`), you can cover dozens of hosts like `www.example.com`, `api.example.com`, and `mail.example.com` using a single cert, which dramatically cuts down on renewals and deployment work.

A Subject Alternative Name (SAN) certificate can also cover multiple names, but you typically have to list each subdomain explicitly. That works, but it's more admin effort when subdomains change or new ones get added. The question says "several dozen subdomains" and they're public-facing, so the simplest ongoing management is usually a wildcard.

Self-signed certificates aren't a good fit for public internet sites because browsers won't trust them by default, causing scary warnings for users. "Domain validation" describes the validation level (DV) of a public certificate, not the coverage type for many subdomains—so it doesn't solve the "lots of subdomains" management problem by itself.

References: https://www.digicert.com/faq/what-is-a-wildcard-certificate and https://letsencrypt.org/docs/faq/

QUESTION NO: 89

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

Explanation:

If the attacker wiped the endpoint logs, you'd pivot to a log source they're less likely to have touched. Firewall logs are perfect for this because they sit at the network edge (or between segments) and record outbound connections from that workstation—destination IPs/domains, ports, timestamps, and whether the traffic was allowed or blocked.

That's exactly what you need when you suspect command-and-control (C2) traffic. Even if the machine's local event logs are gone, the firewall can still show repeated beacons to the same external host, weird ports, or connections at odd hours—classic C2 clues.

An IPS can help, but it's not guaranteed to log everything in a way that's as straightforward for "who talked to what" as a firewall. ACLs are mostly rule sets, not detailed connection histories. And Windows Security logs would have been great—except they were deleted on the endpoint, so you can't rely on them here.

References: https://www.cisa.gov/news-events/news/understanding-firewalls https://attack.mitre.org/tactics/TA0011/

QUESTION NO: 90

Which of the following is a use of CVSS?

A. To determine the cost associated with patching systems

B. To identify unused ports and services that should be closed

C. To analyze code for defects that could be exploited

D. To prioritize the remediation of vulnerabilities

ANSWER: D

Explanation:

CVSS (Common Vulnerability Scoring System) is mainly used to score vulnerabilities so teams can quickly tell what's most serious. The score helps you prioritize what to fix first—something with a higher score (like a critical remote code execution bug) should usually jump to the front of the line compared to a low-impact issue.

It's not about calculating patching costs (that's more of a business/risk budgeting exercise), and it doesn't directly find unused ports/services (that's closer to network scanning and hardening). It also isn't a tool for code analysis—static and dynamic testing tools do that. CVSS is about rating the severity and characteristics of a vulnerability so remediation can be planned sensibly.

References: https://www.first.org/cvss/ and https://nvd.nist.gov/vuln-metrics/cvss

QUESTION NO: 91

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: C E

Explanation:

The biggest thing to nail down first is what threats your organization is actually likely to face. A hospital, a bank, and a manufacturing plant don't get targeted in the same ways, so "one-size-fits-all" training usually misses the mark. If you base the curriculum on industry-specific threat vectors (like phishing, ransomware, or business email compromise), the training feels relevant and people are more likely to remember it and apply it.

The next key piece is the cadence and duration of the training. Security awareness isn't something people learn once and magically keep forever. Short, regular sessions (plus quick refreshers) tend to stick much better than a single long annual presentation. Planning the timing and length up front helps you build a program that people will actually complete and retain.

Other choices can be useful, but they're not the top priorities when you're designing the overall curriculum. For example, secure software development training is great—but it's mainly for developers, not "all personnel."

References: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-awareness-program https://www.nist.gov/privacy-framework/nist-sp-800-50

QUESTION NO: 92

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing

B. Incremental backups

C. UPS

D. RAID

E. Dual power supply

F. NIC teaming

ANSWER: A D

Explanation:

For the "high consumer load" part, **load balancing** is the best fit. It spreads POS traffic across multiple servers, which helps prevent one box from getting overwhelmed during holiday spikes. If a server dies or slows down, the load balancer can route users to healthier systems, keeping the site up.

For "server-data fault tolerance," **RAID** is the clear winner. RAID (like RAID 1/10) protects against a single drive failure by mirroring or using parity, so the server can keep running and data stays available even if a disk drops out. That's directly aimed at avoiding outages caused by storage failures.

The other options don't hit both goals as well: incremental backups help with recovery, not real-time availability; a UPS and dual power supplies help with power issues only; and NIC teaming improves network link resilience but doesn't address the "data fault tolerance" requirement as directly as RAID.

References: https://www.cloudflare.com/learning/performance/what-is-load-balancing/ and https://www.ibm.com/docs/en/ts3500-tape-library?topic=overview-raid

QUESTION NO: 93

A company's website is www.company.com. Attackers purchased the domain www.c0mpany.com. Which of the following types of attacks describes this example?

A. Typosquatting

B. Brand impersonation

C. On-path

D. Watering-hole

ANSWER: A

Explanation:

This is a classic case of **typosquatting**. The attacker registers a look-alike domain (in this case swapping the letter “o” with the number “0”) and hopes users won’t notice the difference when they type or click a link. If someone lands on the fake site, the attacker can steal logins, collect payment info, or drop malware.

While it does involve pretending to be the company, “brand impersonation” is a broader idea. The specific trick here is abusing a tiny spelling/character change in the domain name, which is exactly what typosquatting (also called a look-alike domain attack) means.

“On-path” (man-in-the-middle) would require intercepting traffic between the user and the real site, and “watering-hole” is when attackers compromise a legitimate site that the victims commonly visit. Neither of those matches buying a near-identical domain.

References: https://www.icann.org/resources/pages/phishing-2017-06-20-en and https://www.cloudflare.com/learning/security/glossary/what-is-typosquatting/