CompTIA Security+ SY0-701 Certification

260+ Questions Explained

Thank you for choosing this resource! This comprehensive material has been designed to provide you with over 260 questions, complete with correct answers and detailed explanations, to help you prepare effectively for the CompTIA Security+ SY0-701 exam.

While this resource is an excellent starting point and reference for your exam preparation, please note that it does not substitute the official book and other primary resources. Instead, it serves to clarify and reinforce key concepts, offering a deeper understanding of the exam objectives, backed by official sources and practical advice to help you succeed on your first attempt.

I aim to make these notes accessible to everyone. If you find them helpful, your support through tips/comments or contributions is always appreciated.
It enables me to continue creating high-quality study materials.

✓ Check this post for access to additional valuable resources, such as correct questions with explanations, a glossary, and study methods to help you pass the exam: linkedin.com/in/matteoschirinzi

Comment & like the post of Sec+ resource with your experience: linkedin.com/in/matteoschirinzi

Thank you for your support and good luck on your journey to earning the CompTIA Security+ certification!

1- Which of the answers listed below can be used to describe operational security controls (Select 3 answers)

- Also known as administrative controls
- Focused on the day-to-day procedures of an organization
- Executed by computer systems (instead of people)
- Used to ensure that the equipment continues to work as specified
- Focused on managing risk
- Primarily implemented and executed by people (as opposed to computer systems)

2- What are the examples of preventive security controls? (Select 3 answers)

- Encryption
- IDS
- Sensors
- Firewalls
- Warning signs
- AV software -> Ativirus software

3- Examples of deterrent security controls include: (Select 3 answers)

- Warning signs
- Sensors
- Lighting Proper lighting increases visibility and reduces the chances of unauthorized activity by making it harder to act unnoticed.
- Video surveillance
- Security audits
- Fencing/Bollards

4- Which of the answers listed below refer(s) to detective security control(s)? (Select all that apply)

- Lighting
- Log monitoring
- Sandboxing
- Security audits
- CCTV
- IDS
- Vulnerability scanning

5- Which of the following answers refer(s) to corrective security control(s)? (Select all that apply)

- Recovering data from backup copies
- Applying software updates and patches to fix vulnerabilities
- Developing and implementing IRPs to respond to and recover from security incidents
- Regularly reviewing logs for anomalies or patterns indicative of attacks
- Activating and executing DRPs to restore operations after a major incident

(**Incident Response Plans (IRPs) e Disaster Recovery Plans (DRPs)**)

6- Which of the answers listed below refer(s) to compensating security control(s)? (Select all that apply)

- Backup power systems (Your answer)
- Video surveillance
- MFA (Missed)
- Application sandboxing (Your answer)
- Network segmentation (Missed)

7- Which of the following terms fall into the category of directive security controls? (Select 2 answers)

- IRP (Your answer)
- AUP (Missed)
- IDS
- MFA (Your answer)
- IPS

(**AUP (Acceptable Use Policy)** – A document that specifies acceptable and unacceptable behaviors when using organizational resources.)

8- The term "Non-repudiation" describes the inability to deny responsibility for performing a specific action. In the context of data security, non-repudiation ensures data confidentiality, provides proof of data integrity, and proof of data origin.

- True (Your answer)
- False (Missed)

(While non-repudiation does ensure proof of data origin and integrity (by verifying that the data comes from the stated sender and has not been altered), it **does not** directly ensure **data confidentiality**)

9- Which type of user account violates the concept of non-repudiation?

- Standard user account
- Shared account (Missed)
- Guest user account (Your answer)
- Service account

(A shared account is used by multiple users, which violates the concept of non-repudiation. Non-repudiation requires that actions can be attributed to a single, identifiable user)

10- The term "Zero Trust security" refers to a cybersecurity model that eliminates implicit trust from networks and requires all users and devices to be continuously verified before being granted access to resources. The implementation of the Zero Trust security involves two distinct components: a Data Plane, responsible for defining and managing security policies, and a Control Plane, responsible for enforcing the security policies established by the Data Plane.

- True
- False

The **Data Plane** and **Control Plane** roles in the description are reversed. In a Zero Trust security model:

- **Control Plane**: Defines and manages security policies (policy decisions).
- **Data Plane**: Enforces the security policies established by the Control Plane (policy enforcement)

11- What are the key components of the Zero Trust Control Plane's Policy Decision Point (PDP)? (Select 2 answers)

- Policy Engine (PE)
- Monitoring and logging
- Policy Enforcement Point (PEP)
- Microsegmentation
- Policy Administrator (PA)

Explanation:

- **Policy Engine (PE)**: Responsible for making decisions about whether a user or device should be granted access to a resource, based on security policies.
- **Policy Administrator (PA)**: Enforces the decisions made by the Policy Engine by configuring the Policy Enforcement Points (PEPs) to allow or block access.

Incorrect Answers:

- **Monitoring and Logging**: Important for auditing and visibility but not part of the PDP.
- **Policy Enforcement Point (PEP)**: Part of the Data Plane, not the Control Plane or PDP.
- **Microsegmentation**: A security strategy used to isolate resources but not directly part of the PDP.

12- A honeyfile can be used for:

- Attracting cyber attackers
- Triggering alerts when accessed
- Monitoring network activity
- All of the above

A **honeyfile** is a decoy file designed to detect unauthorized access and gather intelligence about potential attackers

13- Which of the answers listed below refers to software technology designed to provide confidentiality for an entire data storage device?

- TPM
- FDE
- EFS
- HSM

FDE (Full Disk Encryption): A software technology designed to encrypt the entire contents of a storage device to ensure confidentiality. It protects data at rest, even if the device is lost or stolen.

14- An MS Windows component that enables encryption of individual files is called:

- SED
- EFS
- BitLocker
- FDE

EFS (Encrypting File System): A Microsoft Windows feature that allows users to encrypt individual files or folders on an NTFS-formatted drive, providing confidentiality at the file level.

15- Which of the following software application tools are specifically designed for implementing encryption algorithms to secure data communication and storage? (Select 2 answers)

- VPN
- GPG
- SSH
- IPsec
- PGP

GPG (GNU Privacy Guard): A free encryption software that implements the OpenPGP standard to encrypt and sign data and communications securely.
PGP (Pretty Good Privacy): A widely used encryption program for securing emails, files, and data storage using encryption and signing.

16- Which of the answers listed below refers to a deprecated TLS-based method for secure transmission of email messages?

- S/MIME
- STARTTLS
- DKIM
- SMTPS

SMTPS (Simple Mail Transfer Protocol Secure): A deprecated method for transmitting email messages securely over TLS. It used a dedicated port (port 465) for encrypted communication but has been largely replaced by STARTTLS, which upgrades an existing unencrypted connection to use encryption.

17- Which of the following answers refers to an obsolete protocol used for secure data transfer over the web?

- SMTPS
- SRTP (Your answer)
- SHTTP (Missed)
- S/MIME

SHTTP (Secure Hypertext Transfer Protocol): An obsolete protocol used for secure data transfer over the web. It was designed to secure individual messages, but it has been replaced by HTTPS, which provides more robust security at the transport layer.

18- SFTP is an extension of the FTP protocol that adds support for SSL/TLS encryption.

- True (Your answer)
- False (Missed)

SFTP (Secure File Transfer Protocol) is not an extension of FTP. Instead, it is based on **SSH (Secure Shell)** for secure file transfer. The protocol that adds SSL/TLS encryption to FTP is **FTPS (FTP Secure)**, not SFTP.

19- An encryption protocol primarily used in Wi-Fi networks implementing the WPA2 security standard is called:

- TKIP (Your answer)
- CCMP (Missed)
- SSL
- Ipsec

Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is the encryption protocol used in **WPA2** security. It is based on **AES (Advanced Encryption Standard)** and provides strong security compared to the older **TKIP (Temporal Key Integrity Protocol)** used in WPA.

20- A security protocol designed to improve the security of existing WEP implementations is known as:

- WPA2 (Your answer)
- RC4
- CCMP
- TKIP (Missed)

TKIP was designed as an **interim security enhancement** for **WEP (Wired Equivalent Privacy)** before WPA2 was widely adopted. It introduced features like per-packet key mixing, message integrity checks, and rekeying mechanisms to improve WEP security without requiring new hardware.

21- Which of the following answers refer(s) to deprecated/insecure encryption protocols and cryptographic hash functions? (Select all that apply)

- DES (Your answer)
- AES-256
- MD5 (Missed)
- ECC (Your answer)
- SHA-1 (Your answer)
- SSL (Missed)
- RC4 (Missed)

✓ **DES** → **Deprecated** (Weak 56-bit key, vulnerable to brute-force attacks)

✓ **MD5** → **Insecure** (Prone to collisions, not recommended for cryptographic security)

✓ **SHA-1** → **Deprecated** (Collision vulnerabilities, replaced by SHA-2 and SHA-3)

✓ **SSL** → **Deprecated** (Replaced by TLS due to security vulnerabilities)

✓ **RC4** → **Insecure** (Weaknesses allow practical attacks, no longer recommended)

Explanation of the other options:

- **AES-256** → **Secure** (Strong encryption standard used in modern cryptography)
- **ECC (Elliptic Curve Cryptography)** → **Secure** (Modern and efficient cryptographic approach)

22- Which cryptographic protocol is designed to provide secure communications over a computer network and is the successor to SSL?

- IPsec (Your answer)
- TLS (Missed)
- AES
- CCMP

TLS is the **successor to SSL (Secure Sockets Layer)** and is used to provide secure communication over computer networks, such as HTTPS for websites. TLS improves upon SSL by offering stronger encryption, authentication, and integrity protection.

23- Which of the algorithms listed below are not symmetric ciphers? (Select 3 answers)

- AES
- DES
- DHE (Missed)
- ECC (Your answer)
- IDEA
- RC4 (Your answer)
- RSA (Your answer)

24- Which of the following algorithms do(es) not fall into the category of asymmetric encryption? (Select all that apply)

- AES (Your answer)
- DES (Your answer)
- DHE (Your answer)
- ECC
- IDEA (Your answer)
- RC4 (Missed)
- RSA

25- Which of the following answers refers to a protocol used to set up secure connections and exchange of cryptographic keys in IPsec VPNs?

- SSL
- IKE (Missed)
- ESP
- DHE (Your answer)

IKE is the protocol used in **IPsec VPNs** to establish secure connections and **exchange cryptographic keys** between devices. It handles authentication and negotiates security associations (SAs) to ensure a secure communication channel.

26- Which of the answers listed below refers to a key exchange protocol that generates temporary keys for each session, providing forward secrecy to protect past and future communications?

- PFS (Your answer)
- SHA
- PGP
- DHE (Missed)

DHE (Diffie-Hellman Ephemeral) is a **key exchange protocol** that generates **temporary session keys** for each communication session. This provides **forward secrecy**, meaning that even if a session key is compromised, past and future communications remain secure.

27- Which of the following answers refers to a cryptographic key exchange protocol that leverages ECC for enhanced security and efficiency?

- IKE (Your answer)
- ECDHE (Missed)
- DHE
- ECDSA

ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) ECDHE is a **key exchange protocol** that uses **Elliptic Curve Cryptography (ECC)** to provide **enhanced security and efficiency** compared to traditional Diffie-Hellman (DHE). It supports **Perfect Forward Secrecy (PFS)**, ensuring that past communications remain secure even if a private key is compromised

28- Which of the answers listed below refers to a solution designed to strengthen the security of session keys?

- ECB (Your answer)
- PFS (Missed)
- EFS
- PFX

Perfect Forward Secrecy (PFS) strengthens the security of **session keys** by ensuring that each session key is **independent** and **not derived from a long-term key**. This means that even if a private key is compromised, past and future session keys remain secure.

29- Which cryptographic solution would be best suited for low-power devices, such as IoT devices, embedded systems, and mobile devices?

- ECC (Missed)
- DES
- RSA
- AES (Your answer)

ECC (Elliptic Curve Cryptography) is the best cryptographic solution for **low-power devices** like **IoT devices, embedded systems, and mobile devices** because it provides **strong security with smaller key sizes** compared to RSA and AES. This results in **lower computational overhead**, reduced power consumption, and faster encryption/decryption operations—ideal for resource-constrained environments.

30- A block cipher mode that combines a unique counter with encryption key to generate a stream of pseudorandom data blocks which are then used for encrypting data is called:

- CBC (Your answer)
- GCM
- CFB
- CTM (Missed)

CTR mode (Counter Mode) works by using a unique counter value (nonce + counter) combined with the encryption key to generate a keystream. This keystream is then XORed with the plaintext to produce ciphertext.

31- Which of the block cipher modes listed below is the simplest/weakest and therefore not recommended for use?

- CBC (Your answer)
- GCM
- ECB (Missed)
- CTM

ECB is the weakest block cipher mode because it encrypts each block of plaintext independently using the same key

32- Which block cipher mode combines CTM for encryption with an authentication mechanism to ensure both data confidentiality and integrity?

- CBC
- GCM (Missed)
- ECB (Your answer)
- CFB

GCM combines Counter Mode (CTR) encryption with authentication, ensuring both confidentiality and integrity.

33- Which of the following answers refers to an embedded microcontroller used for secure boot, disk encryption, and system integrity verification?

- TPM (Missed)
- SoC
- UEFI (Your answer)
- HSM

A **TPM (Trusted Platform Module)** is a specialized embedded microcontroller designed for security functions like: **Secure Boot**, **Disk Encryption**, **System Integrity Verification**

34- Which of the answers listed below refers to a piece of hardware and associated software/firmware designed to provide cryptographic and key management functions?

- EFS
- HSM (Missed)
- SFC
- TPM (Your answer)

An **HSM (Hardware Security Module)** is a dedicated piece of hardware that provides **cryptographic operations** and **secure key management** functions. It is commonly used in enterprises, cloud security, and financial institutions

35- Which of the following answers refers to a centralized server that is used to distribute cryptographic keys and authenticate users and services within a computer network?

- PKI (Your answer)
- RAS
- KDC (Missed)
- NAS

A **Key Distribution Center (KDC)** is a centralized server that handles **cryptographic key distribution** and **authentication** in a network. It is commonly used in **Kerberos authentication**

36- In a Kerberos-protected network, this type of secure token is granted to users during their initial login to enable them access to multiple network services without the need to re-enter their login credentials.

- OTP (Your answer)
- TGT (Missed)
- AS
- TGS

The correct answer is **TGT (Ticket Granting Ticket)**
In a **Kerberos-protected network**, when a user logs in:

1. The **Authentication Server (AS)** verifies the user's credentials.
2. The AS **issues a TGT (Ticket Granting Ticket)**, which is encrypted and only readable by the Ticket Granting Server (TGS).
3. The user presents the TGT to the **TGS (Ticket Granting Server)** whenever they need access to a network service.
4. The TGS then provides **service tickets**, allowing access **without re-entering credentials**.

37- Which of the answers listed below refers to a cryptographic hash function that has been widely used in the past but is now considered deprecated for security-sensitive applications due to known vulnerabilities?

- MD5 (Missed)
- SHA (Your answer)
- CRC
- HMAC

MD5 was widely used in the past for **hashing passwords, integrity checks, and digital signatures**, but it is now **deprecated** for security-sensitive applications. While **SHA-1 is also deprecated**, **SHA-256 and higher (SHA-2, SHA-3)** are still secure and widely used

38- Which of the following answers refer to algorithms used for generating and verifying digital signatures? (Select 3 answers)

- ECDSA (Missed)
- RSA (Your answer)
- ECDHE (Your answer)
- DSA (Your answer)
- GPG/PGP

39- Which of the answers listed below refer to DSA? (Select 3 answers)

- Asymmetric algorithm (Your answer)
- Used for the key exchange process (Your answer)
- Symmetric algorithm
- Provides authentication, integrity, and non-repudiation (Missed)
- Specifically designed for creating and verifying digital signatures (Your answer)
- Used for encryption

40- Which of the answers listed below describe(s) the characteristics of ECDSA? (Select all that apply)

- Provides authentication, integrity, and non-repudiation (Missed)
- Based on elliptic curve cryptography (Your answer)
- Designed for data encryption
- Specifically designed for creating and verifying digital signatures (Your answer)
- More computationally efficient than other signature algorithms (Missed)
- Enables the key exchange process (Your answer)

41- Given the computational limitations of IoT devices, smartcards, and mobile devices, which of the following digital signature algorithms would be the most efficient choice due to its smaller key size and lower processing requirements?

- RSA
- ECDHE
- DSA
- ECDSA (Missed)
- ECC (Your answer)

42- Key stretching is a cryptographic technique that enhances the security of sensitive data, such as cryptographic keys and passwords. It works by repeatedly applying a resource-intensive function or algorithm to the input data, thus increasing the computational effort required to derive the original key or password, which makes the data more resistant to brute-force, dictionary, or rainbow table attacks.

- True (Missed)
- False (Your answer)

Key stretching is indeed a cryptographic technique that strengthens the security of passwords or keys by making the process of brute-forcing or cracking them more difficult. This is achieved by repeatedly applying a **resource-intensive function** (such as PBKDF2, bcrypt, or scrypt) to the input data (like a password or cryptographic key). As a result, even if an attacker gains access to the hashed or encrypted data, the increased computational effort makes it much harder to recover the original data through attacks like brute force, dictionary, or rainbow table attacks.

43- Which of the answers listed below refers to a set of standards and specifications that define various cryptographic techniques, including formats for public keys, private keys, digital signatures, and digital certificates?

- ITIL
- RFC (Your answer)
- PKCS (Missed)
- ISO/IEC

PKCS (Public Key Cryptography Standards) is a set of standards and specifications developed by RSA Laboratories that defines various cryptographic techniques and formats for public keys, private keys, digital signatures, and digital certificates.

44- Which of the following defines a file format for storing and exchanging personal identity information, including private keys and digital certificates?

- P10 (Your answer)
- P11
- P12 (Missed)
- P13

P12 (often referred to as **PKCS #12**) defines a **file format** used for storing and exchanging **personal identity information**, including **private keys**, **public keys**, and **digital certificates**. It is widely used for securely storing certificates and private keys in a single, encrypted file.

45- What is the role of Registration Authority (RA) in PKI? (Select 2 answers)

- Accepting requests for digital certificates (Missed)
- Validating digital certificates (Your answer)
- Authenticating the entity making the request (Missed)
- Providing backup source for cryptographic keys
- Issuing digital certificates (Your answer)

46- Which digital certificate type allows to secure multiple domain names or subdomains with a single certificate?

- Extended Validation (EV) certificate
- Wildcard certificate
- Subject Alternative Name (SAN) certificate (Missed)
- Root signing certificate (Your answer

A SAN certificate allows you to secure multiple domain names or subdomains under a single certificate. This is ideal for businesses or websites that need to manage multiple domains without needing separate SSL certificates for each one.

47- Choose an answer from the drop-down list on the right to match a threat actor type on the left with its common attack vector attribute.

Question	Answer	Your answer	Res
Nation-state	External	External	Cor

Question	Answer	Your answer	Res
Unskilled attacker	Internal/External	Internal	Wr
Hacktivist	External	Internal/External	Wr
Insider threat	Internal	Internal	Cor
Organized crime	External	External	Cor
Shadow IT	Internal	Internal	Cor

48- Match each threat actor type with its corresponding resources/funding attribute.

Question	Answer	Your answer
Nation-state	High resources and funding	High resources and funding
Unskilled attacker	Low resources and funding	Low resources and funding
Hacktivist	Low to medium resources and funding	Low to medium resources and funding
Insider threat	Low to high resources and funding	Low to high resources and funding
Organized crime	Medium to high resources and funding	Medium to high resources and funding
Shadow IT	Low to medium resources and funding	Low to high resources and funding

49- Assign the level of sophistication attribute to each threat actor type listed below.

Question	Answer	Your answer
Nation-state	High level of sophistication	High level of sophistication
Unskilled attacker	Low level of sophistication	Low level of sophistication
Hacktivist	Low to medium level of sophistication	Low to high level of sophistication
Insider threat	Low to high level of sophistication	Medium to high level of sophistication
Organized crime	Medium to high level of sophistication	High level of sophistication

Question	Answer	Your answer
Shadow IT	Low to medium level of sophistication	Medium to high level of sophistication

50- From the drop-down list on the right, select the typical motivations behind the actions of each threat actor type.

Question	Answer	Your answer
Nation-state	Espionage, political/philosophical beliefs, disruption/chaos, war	Espionage, political/philosophical beliefs, disruption/chaos, war
Unskilled attacker	Disruption/chaos, financial gain, revenge	Financial gain, data exfiltration, extortion
Hacktivist	Ethical beliefs, philosophical/political beliefs, disruption/chaos	Ethical beliefs, philosophical/political belie disruption/chaos
Insider threat	Revenge, financial gain, service disruption	Revenge, financial gain, service disruption
Organized crime	Financial gain, data exfiltration, extortion	Disruption/chaos, financial gain, revenge
Shadow IT	Convenience, lack of awareness of security risks, meeting specific needs	Convenience, lack of awareness of security meeting specific needs

51- Which of the following terms is used to describe sophisticated and prolonged cyberattacks often carried out by well-funded and organized groups, such as nation-states?

- MitM (Your answer)
- APT (Missed)
- XSRF
- DDoS

APT (Advanced Persistent Threat): An **APT** refers to sophisticated, prolonged cyberattacks that are usually conducted by well-funded and organized groups, such as nation-states or cybercriminal organizations. These attacks are designed to infiltrate networks, maintain long-term access, and exfiltrate sensitive data without detection.

52- Which of the answers listed below refers to an email-based threat vector?

- Spoofing
- Phishing (Your answer)
- BEC attacks
- Malicious links
- Malware attachments

- All of the above (Missed)

53- Examples of threat vectors directly related to the use of removable devices include: (Select 2 answers)

- Pretexting
- Malware delivery (Your answer)
- Watering hole attacks
- Data exfiltration (Missed)
- Social engineering attacks (Your answer)

❌ Pretexting – This is a social engineering technique where an attacker fabricates a scenario to trick victims into providing information. It's not directly related to removable devices.

❌ Watering hole attacks – This involves compromising a legitimate website to infect users who visit it, rather than using physical removable devices.

❌ Social engineering attacks – While social engineering can be used to convince someone to insert a USB device, the attack itself is not specific to removable devices.

54- Which of the answers listed below refer(s) to client-based software threat vector(s)? (Select all that apply)

- Drive-by download via web browser (Missed)
- Malicious macro (Your answer)
- Vulnerability in a network protocol or device
- USB-based attack (Missed)
- Infected executable file (Your answer)
- Malicious attachment in email application (Your answer)

55- Which of the following answers refer to agentless software threat vectors? (Select 2 answers)

- Phishing email
- Malicious USB drive (Your answer)
- Network protocol vulnerability (Your answer)
- Infected macro
- Packet sniffing (Missed) -> Since no malicious software is installed on the target system, it is considered an agentless threat vector.

56- Exploiting known vulnerability is a common threat vector for:

- Legacy systems/apps (Your answer)
- Unsupported systems/apps (Missed)
- Newly released systems/apps
- Systems/apps with zero-day vulnerability

Unsupported systems/apps: These systems no longer receive security updates, making them vulnerable to previously discovered exploits.

57- Which of the wireless technologies listed below are considered potential threat vectors and should be avoided due to their known vulnerabilities? (Select all that apply)

- WPS (Your answer)
- WAP
- WPA (Your answer)
- WAF
- WPA2 (Missed)
- WEP (Your answer) ⍰

❌ **WAP (Wireless Application Protocol)**: Not a Wi-Fi security protocol, but a standard for mobile network communication.

❌ **WAF (Web Application Firewall)**: Not related to wireless security; it protects web applications from attacks.

58- Which of the following answers refers to a threat vector characteristic only to wired networks?

- ARP Spoofing -> it can also be used in wireless environments
- VLAN hopping -> it can also be used in wireless environments
- Cable tapping (Missed)
- Port sniffing -> it can also be used in wireless environments (wireshark, tcpdump)
- All of the above (Your answer)

59- Which of the following would be the best solution for a company that needs IT services but lacks any IT personnel?

- MSA (Your answer)
- MaaS
- MSP (Missed) -> Managed Service Provider
- MSSP

MSA (Master Service Agreement): An MSA is a **contract** that outlines terms between a company and a service provider but does not provide IT services itself.
MaaS (Monitoring as a Service): MaaS focuses only on monitoring systems (e.g., cybersecurity, network performance) and does not cover full IT management.
MSSP (Managed Security Service Provider): MSSPs specialize in **security services** (e.g., threat detection, firewall management) but do not provide general IT support like an MSP.

60- Which of the following answers refer to common threat vectors that apply to MSPs, vendors, and suppliers in the supply chain? (Select 2 answers)

- Compliance violations (Your answer)
- Brand reputation damage
- Propagation of malware (Missed)
- Operational disruptions (Your answer)
- Social engineering techniques (Missed)

61- A BEC attack is an example of:

- Smishing
- Phishing (Missed)
- Vishing
- Pharming (Your answer)

BEC (Business Email Compromise) is a type of phishing attack where attackers impersonate a trusted figure within a company (like an executive or employee) to deceive others into transferring money or sensitive information. It primarily uses email as the medium, making it a form of phishing.

62- Which type of application attack relies on introducing external code into the address space of a running program?

- Buffer overflow (Your answer)
- Memory injection (Missed)
- Replay attack
- Pointer dereference

Memory injection: type of attack involves injecting malicious code into the memory space of a running program, allowing the attacker to execute arbitrary code or take control of the application.

63- A collection of precompiled functions designed to be used by more than one Microsoft Windows application simultaneously to save system resources is known as:

- DLL (Missed)
- API
- EXE
- INI (Your answer)

DLL (Dynamic Link Library):is a collection of precompiled functions or code that can be used by multiple applications simultaneously. It allows different programs to share common code, saving system resources and making software development more efficient.

64- A type of exploit in which an application **overwrites** the contents of a memory area it should not have access to is called:

- DLL injection
- Buffer overflow (Missed)
- Memory leak (Your answer)
- Privilege escalation

65- A malfunction in a **preprogrammed** sequential access to a **shared resource** is described as:

- Race condition (Missed)
- Concurrency error (Your answer)
- Multithreading
- Synchronization error

66- A type of vulnerability where the state of a resource is verified at one point in time but may change before the resource is actually used is referred to as:

- TOC -> **TOC** is only part of the term and doesn't fully describe the vulnerability.

- TOC/TOU (Missed) -> Time-of-check to time-of-use
- TOU -> refers only to the "time-of-use" part, but the also involves the "time-of-check"
- TSIG ->**Transaction Signature** is a security mechanism used for securing DNS transactions

This vulnerability occurs when a resource is checked for a certain state (time-of-check) and then used later (time-of-use), but the state of the resource might have changed in the meantime. This can lead to race conditions or unauthorized access if the state has been altered between the two points in time.

67- Which of the following answers refers to a virtualization-related vulnerability where virtualized assets allocated to one VM are improperly isolated and can be accessed or compromised by another VM?

- Resource reuse (Missed)
- Privilege escalation
- Resource exhaustion
- Concurrent session usage (Your answer)

In a virtualized environment, multiple virtual machines (VMs) share the same physical hardware. If resources (e.g., memory, storage, or CPU) allocated to one VM are not properly isolated, another VM could potentially access or compromise those resources. This type of vulnerability is referred to as "Resource reuse" because it involves one VM reusing or accessing assets that should have been securely isolated.

68- Which of the answers listed below refer to the characteristic features of bloatware? (Select 3 answers)

- Pre-installed on a device by the device manufacturer or retailer (Missed)
- Generally considered undesirable due to negative impact on system performance (Your answer)
- Installed without user consent (Missed)
- Can be pre-installed, downloaded, or bundled with other software (Your answer)
- Generally considered undesirable due to negative impact on system performance, privacy, and security (Your answer)

Bloatware refers to unnecessary or unwanted software that comes pre-installed on a device, negatively affecting performance, security, and user experience. Pre-installed on a device by the device manufacturer or retailer

69- Which of the following answers refer to the characteristics of a PUP? (Select 3 answers)

- Often installed without clear user consent (Missed)
- Can be pre-installed, downloaded, or bundled with other software (Missed)
- Generally considered undesirable due to negative impact on system performance, privacy, and security (Missed)
- Pre-installed on a device by the device manufacturer or retailer
- Generally considered undesirable due to negative impact on system performance

A **Potentially Unwanted Program (PUP)** is software that a user **may not have intentionally installed** and is often bundled with other applications. While PUPs are not necessarily malware, they are generally unwanted due to their impact on system performance, security, and privacy

70- Which of the statements listed below apply to the definition of a computer virus? (Select 3 answers)

- A self-replicating computer program containing malicious segment
- Malware that typically requires its host application to be run to make the virus active
- A standalone malicious computer program that replicates itself over a computer network
- Malware that can run by itself without any interaction
- Malicious code that typically attaches itself to an application program or other executable component
- A self-contained malicious program or code that does need a host to propagate itself

A **computer virus** is a type of **malware** that:

- **Requires a host file or application** to attach itself to and spread.
- **Becomes active when the infected file is executed** by the user.
- **Can replicate itself** to spread to other files or systems after activated

71- Remapping a domain name to a rogue IP address is an example of what kind of exploit?

- URL hijacking
- DNS cache poisoning (Missed)
- Domain hijacking (Your answer)
- ARP poisoning

DNS cache poisoning (o **DNS spoofing**) occurs when an attacker **corrupts the DNS cache** of a system or network, causing it to resolve a domain name to a **malicious IP address** instead of the legitimate one

72- When domain registrants due to unlawful actions of third parties lose control over their domain names, they fall victim to:

- Sybil attack
- Domain hijacking (Missed)
- Typosquatting
- URL hijacking (Your answer)

Domain hijacking occurs when a **registrant (owner of a domain) loses control** of their domain name due to the **unlawful actions of third parties**

73- The practice of gaining unauthorized access to a Bluetooth device is known as:

- Phishing
- Bluejacking (Your answer)
- Smishing
- Bluesnarfing (Missed)

Bluejacking: This involves sending unsolicited messages to Bluetooth-enabled devices, usually as a prank or spam. However, it does not involve unauthorized access or data theft**.**

74- Which of the answers listed below refers to RFID vulnerability?

- Spoofing
- Eavesdropping
- RFID cloning (Your answer)
- Data interception
- Replay attack

- DoS attack
- All of the above (Missed)

75- Which wireless attack focuses on exploiting vulnerabilities found in WEP?

- IV attack (Missed)
- War driving
- SSID spoofing (Your answer)
- Bluejacking

An **IV (Initialization Vector) attack** is a cryptographic attack that exploits **vulnerabilities in WEP (Wired Equivalent Privacy)** encryption. WEP uses a **24-bit IV**, which is too short and can be reused, making it susceptible to **key recovery attacks**.

76- Which of the statements listed below apply to the CSRF/XSRF attack? (Select 3 answers)

- Exploits the trust a website has in the user's web browser (Missed)
- A user is tricked by an attacker into submitting unauthorized web requests (Your answer)
- Website executes attacker's requests (Your answer)
- Exploits the trust a user's web browser has in a website (Your answer)
- A malicious script is injected into a trusted website (Your answer)
- User's browser executes attacker's script

CSRF (Cross-Site Request Forgery), also known as **XSRF**, is an attack that forces an authenticated user to perform **unwanted actions on a trusted website** without their consent.

77- Which cryptographic attack relies on the concepts of probability theory?

- Brute-force (Your answer)
- KPA
- Dictionary
- Birthday (Missed)

The Birthday attack leverages probability theory, specifically the **birthday paradox** or **birthday problem**, which states that the probability of two random variables (e.g., hashes) colliding increases as the number of samples grows, even when the sample space is large.

78- A short list of commonly used passwords tried against large number of user accounts is a characteristic feature of:

- Replay attack
- Dictionary attack (Your answer)
- Spraying attack (Missed)
- Birthday attack

A **password spraying attack** involves trying a **small number of commonly used passwords** (e.g., "123456", "password", "qwerty") against a **large number of user accounts** to avoid detection mechanisms like account lockouts. This contrasts with a **dictionary attack**, which typically targets a **single account** with many potential passwords from a precompiled list.

79- A type of forensic evidence that can be used to detect unauthorized access attempts or other malicious activities is called:

- CVE
- IoC (Missed)
- AIS (Your answer)
- OSINT

IoC (Indicator of Compromise) Artifacts such as **unusual log entries, file hashes, IP addresses, or registry modifications** that indicate a security breach or malicious activity. IoCs are used in **digital forensics and incident response (DFIR)** to detect and investigate attacks.

80- Which of the terms listed below refers to a logical grouping of computers that allow computer hosts to function as if they were attached to the same broadcast domain regardless of their physical location?

- VLAN (Missed)
- DMZ
- SNMP community
- VPN (Your answer)

VLAN is a logical grouping of computers that behave as if they are on the same broadcast domain, even if they are physically separated across different network switches. VLANs improve network segmentation, security, and performance by logically isolating traffic.

81- What is the name of a solution that increases the efficiency of IP address space management by allowing network administrators to divide networks into subnets of different sizes?

- DNAT
- VLSM (Missed)
- MPLS
- VLAN (Your answer)

Variable Length Subnet Masking): allows network administrators to **subnet a network into smaller, more efficient subnets of varying sizes** instead of using fixed-size subnets. This helps optimize **IP address allocation** by reducing wasted addresses in networks with different requirements.

82- Which of the following provides granular control over user access to specific network segments and resources based on their assigned roles and permissions?

- EDR
- IAM (Missed)
- AAA (Your answer)
- IPS

Identity and Access Management: provides **granular control** over user access to specific network resources based on their **roles, permissions, and identity**. It includes authentication, authorization, and user lifecycle management, ensuring that users only have access to the resources they are permitted to use

83- Which of the answers listed below refers to a solution that allows for easier management and control of network segmentation policies through software applications?

- VDI
- SDN (Missed)
- VPC
- EDR

SDN allows network administrators to **dynamically define and enforce network segmentation policies through software applications**, making it the best choice for easier management and control.

84- Which of the following policies applies to any requests that fall outside the criteria defined in an ACL?

- Fair access policy (Your answer)
- Implicit deny policy (Missed)
- Transitive trust
- Context-aware authentication

The **implicit deny principle** states that **any request that does not explicitly match an allow rule in an Access Control List (ACL) is automatically denied**. This ensures that only explicitly permitted actions are allowed, enhancing security by defaulting to rejection.

85- Which of the answers listed below refer to the concept of data isolation? (Select 2 answers)

- DLP (Missed)
- SDN (Your answer)
- EFS (Missed)
- SWG (Your answer)
- EDR

Both **DLP (to prevent data leaks) and EFS (to encrypt and restrict access to data)** focus on **data isolation**, making them the right choices.

86- Which of the following provides active network security breach response on an individual computer system?

- NIDS
- HIDS (Your answer)
- NIPS
- HIPS (Missed)

HIPS **monitors, detects, and actively prevents** security breaches **on a specific host**, making it the correct answer

87- A type of document outlining the shared responsibilities between a CSP and its customers for securing and managing data and resources is known as: (Select best answer)

- Service Level Agreement (Your answer)
- Acceptable Use Policy
- Cloud Responsibility Matrix (Missed)
- Master Service Agreement

The CRM clearly **defines security and management responsibilities** between the **CSP and the customer**

88- Which of the terms listed below refers to a method for managing infrastructure resources through scripts and templates?

- IaaS (Your answer)
- ML
- IaC (Missed)
- SDN

IaC (Infrastructure as Code):is the practice of managing and provisioning infrastructure resources using scripts and templates. This allows for automated, repeatable deployment and management of infrastructure through code, making it easier to scale, configure, and maintain resources. Common tools used in IaC include Terraform, CloudFormation, and Ansible.

89- A serverless architecture allows developers to create apps and services without having to manage the required infrastructure resources (such as servers, databases, and storage systems), which are handled by:

- CSP (Missed)
- ISP
- MSP (Your answer) **Managed Service Provider):** typically offers IT support, management, and maintenance services but does not directly handle the underlying infrastructure resources used in serverless architectures.
- IdP

The **Cloud Service Provider (CSP)** manages the infrastructure resources for serverless applications, enabling developers to create apps without worrying about servers, storage, or databases

90- Which of the following provides isolation from external computer networks?

- Network segmentation
- Air gap (Missed)
- Hardware firewall (Your answer)
- Protected cable distribution

An **air gap** physically **isolates** a network from external networks, offering the highest level of security against external attacks.

91- Which of the following refers to a broad term that encompasses various control and automation systems used in industrial settings to control and monitor physical processes and machinery?

- ICS (Missed)
- PLC (Your answer)
- SCADA
- HMI

ICS (industrial control system) is a broad term that encompasses a variety of control and automation systems used to **monitor and control physical processes, machinery, and infrastructure** in industrial settings. It includes **SCADA, PLCs, and other control systems** like DCS (Distributed Control Systems). ICS is used in industries like manufacturing, energy, and utilities

92- Which of the answers listed below refers to a specific type of ICS?

- SoC
- CMS
- SCADA (Missed)
- RTOS

SCADA (Supervisory Control and Data Acquisition) is a specific type of **Industrial Control System (ICS)** used to **supervise and control industrial processes** such as in manufacturing, water treatment, energy, and transportation systems. SCADA systems provide real-time data collection, monitoring, and control of processes.

93- Which of the following answers refers to an OS type characterized by low delay between the execution of tasks required in specific applications, such as in military missile guidance systems or in automotive braking systems?

- Unix-like OS (Your answer)
- SoC
- Firmware
- RTOS (Missed)

RTOS (real time operating system) is specifically built to handle **time-sensitive applications**, ensuring that tasks are executed with predictable and **minimal delays**, which is critical for applications like **military systems or automotive safety features**.

94- Which of the answers listed below refer(s) to embedded systems? (Select all that apply)

- Often designed to operate in real-time or with low latency (Your answer)
- Typically equipped with constrained computing resources and storage (Your answer)
- Designed to perform a single task or a few closely related tasks within a larger system (Missed)
- Often integrated with hardware components like sensors and actuators (Your answer)

95- Which of the following terms can be used to describe a system designed to aim for minimized downtime and uninterrupted operation?

- ICS
- HA (Missed)
- RTOS (Your answer)
- SoC

High Availability (HA) refers to a system design that ensures **minimal downtime** and **uninterrupted operation** by eliminating single points of failure and implementing redundancy mechanisms, such as failover systems, load balancing, and backup power supplies

96- Which failure mode prioritizes security over availability, ensuring that no potentially malicious traffic can get through the device?

- Fail-soft
- Fail-through
- Fail-safe (Your answer)
- Fail-close (Missed)

The **fail-close** mode is a security-focused failure mode that prioritizes security over availability. When a device or system fails in this mode, it **closes connections or access** to ensure that **no potentially malicious traffic** can pass through, even at the cost of reducing availability.

97- Which of the following answers refer to passive network monitoring techniques? (Select 2 answers)

- Network tap (Your answer)
- Trunk port
- Port mirroring (Missed)
- SNMP trap (Your answer)
- Registered port

Both **network tap** and **port mirroring** are **passive** network monitoring techniques that capture traffic without altering or interfering with it, allowing network administrators to monitor traffic flow and diagnose issues safely. **Port mirroring** (also known as SPAN - Switched Port Analyzer) is a technique used in network switches to create a **copy of network traffic** from one or more ports, forwarding it to a monitoring port.

98- A type of hardened server used as a secure gateway for remote administration of devices placed in a different security zone is called:

- C2 server
- Jump server (Missed)
- UC server
- Proxy server

Jump server ✅ (or **bastion host**) is a **hardened server** that acts as a **secure gateway** for remote administration of devices placed in different security zones. It is typically used to access and manage servers or systems in **isolated or highly secure environments**. All remote administrative traffic is routed through the jump server, ensuring that it is monitored and controlled.

C2 server ❌ (Command and Control server) is often associated with malicious activities, where it is used by attackers to control compromised systems or devices remotely. It is not related to secure administration.

UC server ❌ (Unified Communications server) is typically used in business environments to support communication services like VoIP, video conferencing, and messaging. It is not related to remote administration or security zones.

Proxy server ❌ acts as an intermediary between a client and the internet, typically used to mask the client's IP address or cache content for performance. While it provides some security benefits, it does not specifically serve as a **gateway for secure remote administration** of devices in different security zones

99- Which of the answers listed below refers to a solution that simplifies web browser configurations by using predefined rules or scripts to make server selection decisions for specific web traffic?

- PAC (Missed)
- DDNS (Your answer)

- PAM
- NAT

PAC (Proxy Auto-Configuration): a file contains predefined rules or scripts that help a web browser automatically determine which proxy server to use for specific web traffic, simplifying browser configurations.

100- Which of the following provides **passive** network security breach response on an individual computer system?

- HIDS (Missed)
- NIPS
- HIPS (Your answer)
- NIDS

HIDS provides passive network security breach response on an individual computer system by monitoring and analyzing the activity on that specific host for any signs of suspicious behavior or security breaches.

101- In active-active mode, load balancers distribute network traffic across:

- Least utilized servers (Your answer)
- None of the servers
- All servers (Missed)
- Most utilized servers

In **active-active mode**, load balancers distribute network traffic across all available servers to ensure that each server shares the load equally, maximizing resource utilization and availability. This mode provides better fault tolerance and scalability because if one server fails, the others can still handle the traffic.

102- Which of the following EAP methods offers the highest level of security?

- PEAP
- EAP-FAST
- EAP-TLS (Missed)
- EAP-TTLS (Your answer)

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) offers the highest level of security among the options listed. It uses client and server certificates for mutual authentication, making it one of the most secure EAP methods available. The use of certificates ensures a high level of encryption and protection against man-in-the-middle attacks. **EAP-TTLS (Tunneled Transport Layer Security)**: still generally considered to be a step below EAP-TLS in terms of security.

103- Which of the following answers refer to the characteristic features of a Layer 4 firewall? (Select 3 answers)

- Operates at the application layer of the OSI model
- Offers complex (slower) traffic filtering (Your answer)

- Filters traffic based on source/destination IP addresses, ports, and protocol types (e.g., TCP/UDP) (Missed)
- Offers basic (faster) traffic filtering (Missed)
- Operates at the transport layer of the OSI model (Your answer)
- Adds the ability to inspect the contents of data packets in addition to the header information (Your answer)

104- Which of the answers listed below refer to a Layer 7 firewall? (Select 3 answers)

- Offers complex (slower) traffic filtering (Missed)
- Filters traffic based on source/destination IP addresses, ports, and protocol types (e.g., TCP/UDP)
- Operates at the transport layer of the OSI model
- Adds the ability to inspect the contents of data packets in addition to the header information (Your answer)
- Offers basic (faster) traffic filtering (Your answer)
- Operates at the application layer of the OSI model (Your answer)

105- Examples of protocols typically used for implementing secure VPN tunnels include: (Select all that apply)

- IPsec (Your answer)
- SRTP
- TLS (Your answer)
- bcrypt (Your answer)
- L2TP (Missed)

- **IPsec**: IPsec (Internet Protocol Security) is a widely used protocol for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. It is commonly used in Virtual Private Networks (VPNs).
- **TLS (Transport Layer Security)**: TLS is used in securing communication over a computer network, often utilized in SSL/TLS-based VPNs such as OpenVPN.
- **L2TP (Layer 2 Tunneling Protocol)**: L2TP is often combined with IPsec to provide secure VPN connections. L2TP itself does not provide encryption, so it is typically paired with IPsec to ensure confidentiality.
- **SRTP (Secure Real-time Transport Protocol)**: SRTP is used to secure voice and video communications, primarily in applications like VoIP, and is not commonly used for VPNs.
- **bcrypt**: bcrypt is a hashing algorithm used for securely storing passwords, not for implementing secure VPN tunnels.

106- Which VPN type is used for connecting computers to a network? (Select 2 answers)

- Remote access (Missed)
- Intranet-based
- Client-to-site (Your answer)
- Site-to-site
- Extranet-based

107- Which of the answers listed below refers to a hardware or software solution providing secure remote access to networks and resources?

- NAC
- RDP
- SSH (Your answer)
- RAS (Missed)

RAS refers to a hardware or software solution that allows users to securely access a network remotely. It provides remote access to resources and services within an internal network over the internet, often using protocols like VPNs for secure communication. SSH is just a protocol! Not hardware

108- Which of the answers listed below refers to a protocol used to set up secure connections and exchange of cryptographic keys in IPsec VPNs?

- SSL
- IKE (Missed)
- ESP
- DHE (Your answer)

IKE is a protocol used in **IPsec VPNs** to establish secure connections and exchange cryptographic keys. It helps in setting up Security Associations (SAs) and negotiating encryption/authentication parameters between VPN endpoints.

109- An IPsec mode providing encryption only for the payload (the data part of the packet) is referred to as:

- Protected mode
- Tunnel mode (Your answer)
- Transport mode (Missed)
- Safe mode

Transport mode in IPsec encrypts only the **payload** (data part) of the packet while keeping the original IP header intact. It is typically used for **end-to-end communication** between two hosts.

- **Use Transport mode** when securing communication between two devices.
- **Use Tunnel mode** when encrypting traffic between networks (e.g., VPN gateways).

110- Which of the following answers refers to a cybersecurity framework that combines network and security functions into a single cloud-based service?

- SASE (Missed)
- SWG (Your answer)
- CASB
- SD-WAN

SASE (Secure Access Service Edge) is a **cybersecurity framework** that integrates **networking and security** into a **single cloud-based service**. It combines technologies like **SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA)** into a unified solution.

111- The purpose of PCI DSS is to provide protection for:

- Credit cardholder data (Missed)
- Licensed software
- User passwords
- Personal health information (Your answer)

PCI DSS (Payment Card Industry Data Security Standard) is a security standard designed to **protect credit cardholder data**. It applies to businesses that **store, process, or transmit payment card information** to prevent fraud and data breaches.

112- Which of the answers listed below refer(s) to encryption method(s) used to protect data at rest? (Select all that apply)

- FDE (Missed) – Full Disk Encryption
- SED (Missed) - Self Encrypting Drive
- IPsec
- TLS
- VPN
- EFS (Your answer) - Encrypting File System

113- Which of the following answers refer to data masking? (Select 2 answers)

- Replaces sensitive data with fictitious or modified data while retaining its original format (Your answer)
- Allows for data manipulation in environments where the actual values are not needed (Missed)
- Transforms data into an unreadable format using an algorithm and an encryption key
- Creates a unique, fixed-length string from the original data
- Replaces sensitive data with a non-sensitive identifier that has no meaning or value outside the specific system (Your answer)

✔ **"Allows for data manipulation in environments where the actual values are not needed"** → Data masking enables secure use of data in **testing or development** environments where real values are unnecessary.

❌ **"Replaces sensitive data with a non-sensitive identifier that has no meaning or value outside the specific system"** → This describes **tokenization**, not masking. Tokenization replaces data with a token that can be mapped back but has no intrinsic meaning.

114- ACL, FACL, DAC, MAC, and RBAC are all access control mechanisms that can be used to manage user permissions and protect the confidentiality, integrity, and availability of data.

- True (Missed)
- False (Your answer)

ACL, FACL(Filesystem ACL), DAC, MAC, and RBAC are all **access control mechanisms** used to manage user permissions and protect data confidentiality, integrity, and availability (**CIA Triad**).

115- Hardware RAID Level 5: (Select 3 answers)

- Requires at least 2 drives to implement
- Continues to operate in case of failure of more than 1 drive
- Is also known as disk striping with double parity
- Requires at least 3 drives to implement (Missed)
- Offers increased performance and fault tolerance (single drive failure does not destroy the array and lost data can be re-created by the remaining drives) (Missed)
- Requires at least 4 drives to implement
- Is also known as disk striping with parity (Missed)

116- Hardware RAID Level 6: (Select 3 answers)

- Is also known as disk striping with parity
- Requires at least 4 drives to implement (Missed)
- Offers increased performance and fault tolerance (failure of up to 2 drives does not destroy the array and lost data can be re-created by the remaining drives) (Missed)
- Requires at least 3 drives to implement
- Is also known as disk striping with double parity (Missed)
- Continues to operate in case of failure of more than 2 drives
- Requires at least 5 drives to implement

117- Hardware RAID Level 10 (a.k.a. RAID 1+0): (Select 3 answers)

- Requires a minimum of 4 drives to implement (Missed)
- Is referred to as stripe of mirrors, i.e., a combination of RAID 1 (disk mirroring) and RAID 0 (disk striping) (Missed)
- Requires a minimum of 5 drives to implement
- Offers increased performance and fault tolerance (failure of one drive in each mirrored pair of disk drives does not destroy the array) (Missed)
- Requires a minimum of 3 drives to implement
- Continues to operate in case of failure of more than 2 drives
- Is referred to as stripe of mirrors, i.e., a combination of RAID 1 (disk striping) and RAID 0 (disk mirroring)

118- Which of the answers listed below refers to a simulated scenario conducted in a controlled environment, typically involving discussions and planning around hypothetical security incidents?

- Tabletop exercise (Missed)
- Sandboxing (Your answer)
- Threat hunting
- Security awareness training

A **tabletop exercise** is a **simulated security scenario** conducted in a **controlled environment** where participants discuss and plan responses to hypothetical cybersecurity incidents. It is used to test incident

response plans, improve coordination, and identify gaps in security policies **without executing real-world attacks**.

119- Which of the solutions listed below provides redundancy and fault tolerance by dividing tasks into smaller subtasks and distributing them across multiple systems to be **executed simultaneously**?

- Load balancing
- Multitasking (Your answer)
- Clustering
- Parallel processing (Missed)

120- What type of backups are commonly used with virtual machines?

- Incremental backups
- Snapshot backups (Missed)
- Tape backups
- Differential backups (Your answer)

Snapshot backups are commonly used with **virtual machines (VMs)**. A snapshot captures the **state** of a VM at a specific point in time, including its disk, memory, and settings. Snapshots allow for quick backups and restores of VMs without affecting the running system.

121- Which of the following terms refers to a backup strategy that relies on creating and maintaining copies of data in real-time or near real-time on a separate system?

- Mirroring (Your answer)
- Virtualization
- Journaling
- Replication (Missed)

Replication refers to the backup strategy where data is continuously or periodically copied from one system to another, often in **real-time or near real-time**. It ensures that an exact copy of the data is maintained on a separate system, providing redundancy and protecting against data loss.

122- Which of the answers listed below refers to a device designed to supply (and monitor the quality of) electric power to multiple outlets?

- PSU (Your answer): **Power Supply Unit**, for individual devices
- MDF: Distribution frames for network connections, not related to power
- PDU: **Power Distribution Unit**, which manages and distributes power to multiple devices.
- IDF: Distribution frames for network connections, not related to power

123- Which of the following power redundancy solutions would be best suited for providing long-term emergency power during an unexpected main power source outage?

- Dual-power supply (Your answer)
- Standby UPS
- Backup generator (Missed)
- Managed PDU

A **backup generator** is best suited for providing **long-term emergency power** during an unexpected main power source outage. It is capable of supplying power for an extended period, typically until the main power source is restored, or until other long-term power solutions are in place.

❌ **Dual-power supply** *(Your answer)* → A dual-power supply provides redundancy by using two independent power sources, often in server systems, but it doesn't provide long-term emergency power. It's designed for **short-term failover** in case of a primary power failure.

124- Which of the terms listed below is used to describe a foundational level of security configurations and settings required to safeguard a system?

- Logical segmentation
- Secure baseline (Missed)
- Access control levels (Your answer)
- Principle of least privilege

Secure baseline:This refers to the minimum security configurations and settings that should be applied to ensure a system is protected from common vulnerabilities and threats. It acts as a starting point for further security measures and improvements

125- In the context of MDM, the isolation of corporate applications and data from other parts of the mobile device is referred to as:

- Containerization (Missed)
- Storage segmentation
- Virtualization
- Content management (Your answer)

In the context of Mobile Device Management (MDM), **containerization** refers to the isolation of corporate applications and data from other parts of the mobile device. It ensures that business data and apps are kept separate from personal data, offering an additional layer of security and preventing unauthorized access to corporate resources.

126- Which of the answers listed below refer to workstation hardening techniques? (Select 3 answers)

- Hiding administrator accounts (Your answer)
- Regularly applying security patches and updates to the OS and installed software (Your answer)
- Disabling all internet access
- Removing or disabling unnecessary drivers, services, software, and network protocols (Your answer)
- Limiting unauthorized or unauthenticated user access (Missed)

127- Which of the following answers refer(s) to (a) router hardening technique(s)? (Select all that apply)

- Changing default credentials (Your answer)
- Disabling unused services and ports (Your answer)
- Changing device name

- Disabling the broadcasting of the router's SSID (Your answer)
- Implementing regular firmware updates (Your answer)

128- Which of the answers listed below refers to the process of assessing the physical environment, such as the layout of the building, to identify potential sources of interference and determine the optimal placement of a WAP?

- Gap analysis (Your answer)
- Capacity planning
- Site survey (Missed)
- Vulnerability scanning

A **site survey** refers to the process of assessing the physical environment, such as the layout of the building, to identify potential sources of interference, **Gap analysis** focuses on identifying gaps between the current state and desired state in a system or process.

129- An administrator needs to adjust the placement of multiple APs to ensure the best wireless signal coverage for the network. Which of the following would be of help in identifying areas of low signal strength?

- Heat map (Missed)
- Power level controls (Your answer)
- Logical network diagram
- Wi-Fi hotspots

130- A mobile device deployment model that allows employees to use private mobile devices for accessing company's restricted data and applications is known as:

- COPE - Corporate-Owned, Personally Enabled
- BYOD (Missed) - Bring Your Own Device
- MDM (Your answer) - Mobile Device Management
- CYOD - Choose Your Own Device

131- Which of the following solutions would offer the strongest security for a small network that lacks an authentication server?

- WPA3-SAE (Missed)
- WPA2-Enterprise
- WPA2-PSK (Your answer)
- WPA3-Enterprise

WPA3-SAE (Simultaneous Authentication of Equals): offers the strongest security in this case because it replaces the traditional PSK (Pre-Shared Key) method used in WPA2 with a more robust password-based authentication protocol that is resistant to offline dictionary attacks, making it more secure than WPA2-PSK

132- What is the name of the encryption protocol primarily used in Wi-Fi networks implementing the WPA3 security standard?

- AES-CCMP (Your answer)
- CBC-MAC
- AES-GCMP (Missed)
- WPA-TKIP

AES-GCMP (AES Galois/Counter Mode Protocol) is the encryption protocol primarily used in Wi-Fi networks implementing the **WPA3** security standard. It provides stronger security and integrity than the older **AES-CCMP** used in WPA2 by offering better resistance to attacks such as replay and tampering.

133- What are the characteristics of TACACS+? (Select 3 answers)

- Encrypts only the password in the access-request packet
- Combines authentication and authorization (Your answer)
- Encrypts the entire payload of the access-request packet (Your answer)
- Primarily used for device administration (Missed)
- Separates authentication and authorization (Missed)
- Primarily used for network access (Your answer)

TACACS+ (Terminal Access Controller Access-Control System Plus) is a network protocol developed by Cisco that provides centralized authentication, authorization, and accounting (AAA) services for managing device access in a network. It is commonly used for device administration, especially for routers, switches, firewalls, and other network infrastructure components.

134- What are the characteristic features of RADIUS? (Select 3 answers)

- Primarily used for network access (Missed)
- Encrypts the entire payload of the access-request packet
- Combines authentication and authorization (Your answer)
- Encrypts only the password in the access-request packet (Your answer)
- Primarily used for device administration (Your answer)
- Separates authentication and authorization

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) for users who connect to and use a network service. It is commonly used in scenarios such as VPNs, Wi-Fi networks, and dial-up connections, offering a way to manage network access and ensure security.

Feature	RADIUS	TACACS+
Process	Combines authentication & authorization	Separates authentication, authorization, and accounting
Encryption	Encrypts only passwords	Encrypts the entire payload
Primary Usage	Network access (e.g., Wi-Fi, VPN)	Device administration (e.g., routers, switches)
Protocol Type	UDP	TCP
Port Number	1812 (authentication), 1813 (accounting)	49
Flexibility	Less granular control	More granular control (e.g., command-level control)
Reliability	Less reliable (UDP)	More reliable (TCP)

135- Which of the answers listed below refers to an open standard wireless network authentication protocol that enhances security by encapsulating authentication process within an encrypted TLS tunnel?

- PEAP (Missed)
- EAP (Your answer)
- LEAP
- RADIUS

PEAP (Protected Extensible Authentication Protocol): AP enhances security by encapsulating the authentication process within an encrypted **TLS (Transport Layer Security) tunnel**. It is commonly used in **enterprise Wi-Fi networks** to provide secure authentication without exposing user credentials.

136- In computer security, a mechanism for safe execution of untested code or untrusted applications is referred to as:

- Sideloading (Your answer)
- Virtualization
- Sandboxing (Missed)
- Stress testing

Sandboxing is a security mechanism that isolates untrusted or untested code in a **restricted environment**, preventing it from affecting the host system. It is commonly used in cybersecurity to safely execute potentially harmful applications, analyze malware, and enforce security policies.

137- Which of the following answers refers to a Windows-specific feature for handling exceptions, errors, and abnormal conditions in software?

- EPC - Error Processing Code or Execution Protection Code
- SEH (Missed)
- EH (Your answer) - Exception Handling not specific for windows

- EXR - Exception Record

SEH (Structured Exception Handling) is a **Windows-specific** feature that provides a mechanism for handling exceptions, errors, and abnormal conditions in software. It allows programs to catch and handle exceptions in a controlled manner, improving stability and security

138- Which type of software enables monitoring and tracking of mobile devices?

- MDM (Missed)
- GPS (Your answer)
- NFC
- GSM

MDM (Mobile Device Management) is software that allows organizations to **monitor, track, manage, and secure mobile devices** (such as smartphones and tablets). It is commonly used in enterprises to enforce security policies, manage apps, track device locations, and perform remote wipes if a device is lost or stolen

139- Vulnerability scanning: (Select all that apply)

- Identifies lack of security controls (Your answer)
- Actively tests security controls
- Identifies common misconfigurations (Your answer)
- Exploits vulnerabilities (Your answer)
- Passively tests security controls (Your answer)

❌ **Exploits vulnerabilities** → Vulnerability scanning **only detects** vulnerabilities; **exploitation** is done during **penetration testing**

140- Which of the following terms refers to threat intelligence gathered from publicly available sources?

- IoC (Your answer)
- OSINT (Missed)
- RFC
- CVE/NVD

OSINT (Open-Source Intelligence) refers to threat intelligence collected from **publicly available sources**, such as websites, social media, news articles, forums, and public databases. It is commonly used in cybersecurity, intelligence gathering, and threat hunting.

141- Which of the terms listed below refers to a US government initiative for real-time sharing of cyber threat indicators?

- AIS (Missed)
- STIX
- TTP
- CVSS (Your answer)

AIS (Automated Indicator Sharing) is a **U.S. government initiative** led by the **Department of Homeland Security (DHS)** to enable **real-time sharing of cyber threat indicators** between the government and private sector organizations

142- What is STIX?

- A type of vulnerability database (Your answer)
- Common language for describing cyber threat information (Missed)
- US government initiative for real-time sharing of cyber threat indicators
- Transport mechanism for cyber threat information

STIX (Structured Threat Information eXpression) is a standardized framework used to **describe, structure, and share cyber threat intelligence (CTI)** in a machine-readable format. It allows organizations to communicate detailed threat information, such as indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs), and threat actors.

143- What is Exposure Factor (EF) in vulnerability analysis?

- The likelihood that a vulnerability will be exploited in a real-world scenario
- The rate at which vulnerabilities are discovered and reported
- The degree of loss that a realized threat would have on a specific asset (Missed)
- The measure of the potential impact of a vulnerability on an organization's assets (Your answer)

Exposure Factor (EF) in vulnerability analysis represents the **percentage of an asset's value that would be lost** if a specific threat were realized. It is a key component in risk assessment calculations, particularly in the **Single Loss Expectancy (SLE)** formula:

SLE = AssetValue(AV) × ExposureFactor(EF)

144- Which of the answers listed below refer to SIEM? (Select 3 answers)

- Allows different security tools to share data and work together more effectively
- Designed to provide a centralized user interface for accessing collected data (Missed)
- A collection of standards developed by NIST
- Enables real-time threat detection, incident response, and compliance monitoring (Missed)
- A type of security system designed to collect logs and events from various sources (Missed)
- Provides a common language for communicating security information

SIEM (Security Information and Event Management) is a **security solution is primarily used for centralized log collection, real-time security monitoring, and compliance reporting!**

145- An SNMP-compliant device includes a virtual database containing information about configuration and state of the device that can be queried by an SNMP management station. This type of data repository is referred to as:

- MIB (Missed)

- DCS (Your answer)
- NMS
- SIEM

MIB (Management Information Base) is a **virtual database** on an SNMP-compliant device that stores information about the device's configuration and operational state.

146- In SNMP, each node in a MIB is uniquely identified by a(n):

- DSU (Your answer) - Data Set Unit not related
- OID (Missed)
- CSU - Centralized Services Unit not related
- OUI - Organizationally Unique Identifier not related

In **SNMP (Simple Network Management Protocol)**, each node in the **MIB (Management Information Base)** is uniquely identified by an **OID (Object Identifier)**. An OID is a hierarchical identifier used to reference specific objects or data points within the MIB, such as configuration settings, device status, and performance metrics. It follows a tree structure where each branch and leaf node is assigned a unique identifier.

147- Which of the answers listed below refer to filtering techniques that can allow or block access to a site based on its web address? (Select 2 answers)

- SSL/TLS inspection
- URL scanning (Your answer)
- Content categorization (Your answer)
- DNS filtering (Missed)
- Reputation-based filtering

148- What is SELinux?

- A security feature in Linux OSs (Missed)
- A secure boot mechanism implemented in certain Linux distributions
- An open-source web server software
- A Linux distribution (Your answer)

SELinux (Security-Enhanced Linux) is a **security feature** implemented in Linux distributions to enforce **mandatory access control (MAC)** policies. It provides an additional layer of security by restricting programs' access to resources based on defined security policies, reducing the potential damage caused by vulnerabilities and misconfigurations.

149- Which of the following answers refers to a security mechanism imposed by SELinux over system access?

- DAC
- RBAC
- MAC (Missed)
- ABAC

150- FTPS is an extension to the SSH protocol and runs by default on TCP port 22.

- True (Your answer)
- False (Missed)

FTPS (File Transfer Protocol Secure) is an extension to the **FTP** protocol, not **SSH**. It adds **SSL/TLS encryption** to FTP to secure data during transfer. FTPS typically runs on ports **990** (implicit) or **21** (explicit), not **TCP port 22**, which is used by **SSH** (Secure Shell).

151- Which of the following protocols enables secure access and management of emails on a mail server from an email client?

- POP3S (Your answer)
- SMTPS
- IMAPS (Missed)
- S/MIME

IMAPS is the secure version of **IMAP** (Internet Message Access Protocol), which is used for accessing and managing emails stored on a mail server. **IMAPS** uses **SSL/TLS encryption** to secure the communication between the email client and the mail server, ensuring that email data is transmitted securely. It typically operates on **port 993**.

❌ **POP3S (Post Office Protocol 3 Secure):** Similar to **IMAPS**, but POP3 is designed for downloading emails from the server rather than managing them on the server. **IMAPS** allows better interaction with the server.

152- Which of the following answers refers to a policy framework that allows domain owners to specify how email receivers should handle emails that fail authentication checks?

- DKIM
- SPF (Your answer)
- PEM
- DMARC (Missed)

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a **policy framework** that allows domain owners to specify how email receivers should handle emails that fail authentication checks (such as **SPF** and **DKIM**). DMARC helps prevent email spoofing and phishing by defining rules for how mail servers should process emails that do not pass authentication, and it provides reporting for domain owners to monitor potential abuse.

153- Which of the answers listed below refers to an authentication method that enables the signing of an outbound email message with a digital signature?

- SPF
- DKIM (Missed)
- DMARC
- PEM (Your answer)

(DomainKeys Identified Mail) DKIM is an authentication method that **enables the signing of outbound email messages** with a **digital signature**. This signature allows the recipient's mail server to verify that the email was not altered during transmission and that it was sent from an authorized sender

154- Which of the following answers refers to an email authentication mechanism that allows domain owners to specify which IP addresses are authorized to send emails on behalf of their domain?

- DMARC (Your answer)
- PEM
- DKIM
- SPF (Missed)

(Sender Policy Framework) SPF allows **domain owners to specify which IP addresses** are authorized to send emails on behalf of their domain. It helps to prevent email spoofing by verifying that an email sent from a domain is coming from an authorized mail server. When an email is received, the recipient's mail server checks the SPF record in the domain's DNS to ensure the sender's IP is authorized.

155- Which of the answers listed below refers to a cryptographic standard (and a file format) used for the storage and transmission of private keys in email communications?

- PEM (Missed)
- DMARC
- SPF
- DKIM (Your answer)

PEM (Privacy-Enhanced Mail) is both a **cryptographic standard** and a **file format** used for the storage and transmission of **private keys** and **certificates** in email communications

156- Which of the answers listed below refers to a security solution that provides the capability for detection, analysis, response, and real-time monitoring of cyber threats at the device level?

- SWG
- CASB (Your answer)
- EDR (Missed)
- NGFW

EDR (Endpoint Detection and Response) refers to a **security solution** that provides capabilities for **detection, analysis, response, and real-time monitoring** of cyber threats specifically at the **device (endpoint) level**.

157- Which of the following answers refers to a framework for managing access control to digital resources?

- PAM (Your answer)
- SSO
- IAM (Missed)
- MFA

IAM (Identity and Access Management) is a **framework** that provides a comprehensive approach to managing **access control** to digital resources. It includes policies, processes, and technologies that allow organizations to manage users' identities and control their access to systems, applications, and data based on predefined rules.

158- Which of the terms listed below is used to describe the technical process of removing a user's access to an organization's systems and resources?

- De-provisioning (Missed)
- Group Policy
- IAM
- Offboarding (Your answer)

De-provisioning refers to the technical process of **removing a user's access** to an organization's systems, applications, and resources. This typically occurs when an employee leaves the organization or changes roles, and it involves revoking access to ensure security

❌ **Offboarding:** Refers to the overall process of transitioning an employee out of the organization, which may include de-provisioning but also involves other tasks like exit interviews and return of company property.

Since you selected **Offboarding**, remember that **de-provisioning** is the specific term for removing user access to systems and resources!

159- OAuth is an open standard for:

- Auditing
- Authentication (Your answer)
- Authorization (Missed)
- Attestation

160- OpenID Connect is a protocol used for:

- Attestation
- Authorization (Your answer)
- Auditing
- Authentication (Missed)

161- Which of the terms listed below refers to the process of confirming the integrity and compliance status of various components such as devices, software, configurations, and user privileges?

- Attestation (Missed)
- Authentication
- Auditing (Your answer)
- Authorization

Attestation refers to the process of **confirming the integrity and compliance status** of various components, such as devices, software, configurations, and user privileges. It is used to verify that systems and resources are in the desired, secure state and comply with predefined security policies.

162- Which access control model allows for defining granular rules that consider user roles, time constraints, and network access restrictions?

- ABAC (Your answer)
- MAC
- RuBAC (Missed)
- DAC
- RBAC

RuBAC allows for defining granular rules that take into account specific conditions, such as user roles, time constraints, and network access restrictions. It works by applying rules that are evaluated when access requests are made, granting or denying access based on those criteria. RuBAC is specifically designed for situations requiring rules like time, network constraints, and roles.

163- Which access control model defines access control rules with the use of statements that closely resemble natural language?

- DAC
- ABAC (Missed)
- MAC
- RBAC (Your answer)

ABAC allows access control rules to be defined using attributes and conditions, often expressed in a form that can resemble natural language. For example, a rule might state something like: "Allow access to resource X if the user's role is 'manager'

164- Which of the answers listed below refer(s) to a medium type that can be used as a hardware authentication token? (Select all that apply)

- Smart card (Your answer)

- Key fob (Missed)
- Security key (Your answer)
- Passphrase
- Biometric reader (Your answer)
- RFID badge (Your answer)

165- Which of the answers listed below refer to the features of a security key? (Select 3 answers)

- Used for OTP generation, remote vehicle access, and building access (Your answer)
- Hardware authentication token (Your answer)
- Typically, a physical USB stick or key fob-sized device (Your answer)
- Primarily used for digital security (2FA/MFA) (Missed)
- Software authentication token
- Typically, a credit card-sized plastic card with an embedded chip

166- The minimum password age policy setting determines the period of time that a password can be used before the system requires the user to change it.

- True (Your answer)
- False (Missed)

The **minimum password age policy** actually determines the minimum amount of time that must pass before a user can change their password. It does not require a password change after a specific period, but instead prevents users from changing their password too frequently.

167- A security solution that provides control over elevated (i.e., administrative type) accounts is referred to as:

- MFA (Your answer)
- IAM
- SSO
- PAM (Missed)

Privileged Access Management: PAM is a security solution specifically designed to control and monitor elevated or administrative accounts. It helps manage and secure privileged access, ensuring that administrative accounts are used appropriately and reducing the risk of misuse.

168- Which of the answers listed below refers to a solution designed to minimize the risk of unauthorized access to privileged accounts?

- Principle of least privilege (Your answer)
- Just-in-time-permissions (Missed)

- Passwordless authentication
- Multifactor authentication

Just-in-time permissions is a security approach that minimizes the risk of unauthorized access to privileged accounts by granting elevated access only when it is needed and for a limited time. This reduces the time frame in which privileged accounts are accessible, lowering the potential for misuse.

169- Which of the following answers refers to an encrypted database that provides secure storage space for user credentials?

- Secure enclave
- Password manager (Your answer)
- Rainbow table
- Password vault (Missed)

A **password vault** is a secure database specifically designed to store user credentials, such as passwords, in an encrypted format. It provides a safe way to manage and store passwords, often offering features like encryption, password generation, and secure access.

170- Which of the terms listed below refers to a process that deals with coordinating and managing multiple repetitive tasks?

- Sequencing
- Orchestration (Missed)
- Scripting (Your answer)
- Automation

Orchestration refers to the process of coordinating and managing multiple repetitive tasks, often across different systems or services, to ensure they work together efficiently. It goes beyond simple automation by handling dependencies, error management, and optimization of workflows.

171- Which of the following technologies enables automated handling of multiple security incidents?

- SOAP (Your answer) - Simple Object Access Protocol
- SASE
- SOAR (Missed)
- SIEM

SOAR (Security Orchestration, Automation, and Response): platforms enable automated handling of multiple security incidents by integrating security tools, automating workflows, and orchestrating responses to threats. They help security teams improve efficiency and respond to incidents faster

172- Which of the following answers refers to a set of rules, policies, or automated controls designed to regulate technology-related decisions and actions within an organization?

- Technical standards
- Compliance requirements
- Guardrails (Missed)
- Security baselines (Your answer)

Guardrails refer to a set of rules, policies, or automated controls designed to regulate technology-related decisions and actions within an organization. They help ensure security, compliance, and operational efficiency without overly restricting innovation and agility.
Security baselines, refers to predefined security configurations that set minimum security standards for systems and applications but do not necessarily cover broader governance aspects like decision-making and automation that guardrails address.

173- Which of the answers listed below refers to a term primarily used in software development to describe the cost of short-term decisions that can lead to long-term problems?

- Code entropy
- Exposure factor (Your answer)
- Risk register
- Technical debt (Missed)

Technical debt refers to the cost of taking shortcuts or making suboptimal decisions in software development to achieve short-term goals, which can lead to long-term maintenance issues, increased complexity, and higher costs in the future.

174- In the incident response process, the step that involves identifying and understanding potential incidents to determine their scope, impact, and root cause is a part of the:

- Preparation stage (Your answer)
- Detection and analysis stage (Missed)
- Containment, eradication, and recovery stage
- Post-incident activity stage

175- A type of document stipulating rules of behavior to be followed by users of computers, networks, and associated resources is known as:

- SLA (Your answer) **Service Level Agreement** is a contract between a service provider and a customer
- EULA
- AUP (Missed)
- BPA

An **AUP (Acceptable Use Policy)** is a document that outlines the rules and guidelines for users regarding the appropriate use of an organization's computers, networks, and other IT resources. It helps prevent misuse and ensures security and compliance.

176- Which of the following acronyms refers to a comprehensive strategy and set of procedures designed to ensure that an organization can continue its critical operations and functions during and after a disruptive event?

- DRP
- CP
- BCP (Missed)
- COOP (Your answer)

A **Business Continuity Plan (BCP)** is a comprehensive strategy and set of procedures designed to ensure that an organization can maintain critical operations and functions during and after a disruptive event, such as a cyberattack, natural disaster, or system failure
COOP (Continuity of Operations Plan), is related but is more commonly used in government and military contexts to ensure essential functions continue in emergencies. **BCP** is the broader term used across various industries.

177- Which of the answers listed below refers to a set of procedures put in place to recover IT systems and data following a major disruption?

- BCP
- DRP (Missed) – Disaster Recovery Plan
- IRP (Your answer) – Incident Response Plan
- ERP
-

178- Which of the following terms refers to a documented plan outlining the steps that should be taken in each phase of a cybersecurity incident?

- DRP (Your answer)
- IRP (Missed)
- BCP
- ERP

179- Which of the following answers refers to a general term used to describe a specialized group within an organization focusing on specific tasks or areas of responsibility?

- Council
- Advisory board
- Committee (Missed)
- Task force (Your answer)

180- Which of the answers listed below refer(s) to individuals responsible for the day-to-day management, storage, and protection of data? (Select all that apply)

- Processors (Your answer)
- Controllers
- Stewards (Missed)
- Owners

- Custodians (Your answer)

✅ **Stewards** – Data stewards are responsible for the day-to-day management, quality, and governance of data, ensuring it is accurate, consistent, and properly maintained.

✅ **Custodians** – Data custodians are responsible for the storage, protection, and technical management of data, implementing security controls and ensuring compliance with policies.

181- The process of determining potential risks that could affect an organization's ability to achieve its objectives is called:

- Risk assessment (Your answer)
- Risk identification (Missed)
- Risk analysis
- Risk management

• **Risk assessment (Correct Answer)** – This is the overall process of identifying, analyzing, and evaluating risks that could impact an organization's objectives. It includes both risk identification and risk analysis.

• **Risk identification** – A sub-process of risk assessment that focuses specifically on recognizing potential risks. While important, it is not the complete process.

182- The process of evaluating discovered risks to understand their potential impact and likelihood is referred to as:

- Risk analysis (Your answer)
- Risk assessment (Missed)
- Risk identification
- Risk management

183- Which of the answers listed below refers to an example of continuous risk assessment?

- Quarterly or annual risk assessments (Your answer)
- Risk assessment for a new product launch
- Assessing risk after a major organizational change or a security breach
- Real-time monitoring of network security threats (Missed)

184- Which of the following terms is used to describe the predicted loss of value to an asset based on a single security incident?

- SLE (Missed) – Single Loss Expectancy SLE=AssetValue×ExposureFactor(EF)
- ARO - Annualized Rate of Occurrence

- ALE (Your answer) - Annualized Loss Expectancy ALE=SLE×ARO
- SLA - Service Level Agreement

185- Which of the acronyms listed below refers to a risk assessment formula defining probable financial loss due to a risk over a one-year period?

- ARO
- SLE (Your answer)
- ALE (Missed)
- SLA

186- Which of the following answers refers to the correct formula for calculating probable financial loss due to a risk over a one-year period?

- SLE = AV x EF
- ALE = ARO x SLE (Missed)
- SLE = ALE x AV (Your answer)
- ALE = AV x EF

187- In quantitative risk assessment, this term is used for estimating the likelihood of occurrence of a future threat.

- ALE (Your answer)
- SLA
- ARO (Missed)
- SLE

188- Which of the following terms is used to describe the specific level of risk an organization is prepared to accept in pursuit of its objectives?

- Risk appetite
- Risk tolerance (Missed)
- Risk acceptance
- Risk capacity (Your answer)

Risk tolerance: refers to the specific level of risk an organization is willing to accept within its overall **risk appetite**. It defines acceptable variations in risk levels while still pursuing objectives

Risk capacity: refers to the maximum amount of risk an organization is able to handle, considering financial and operational constraints. It is different from the level of risk an organization is **willing** to take

189- Which of the terms listed below refers to a general term that describes an organization's overall attitude towards risk-taking?

- Risk strategy
- Risk control
- Risk appetite (Missed)
- Risk tolerance (Your answer)

Risk appetite – A broader concept that describes the overall amount of risk an organization is willing to take on to achieve its goals. **Risk tolerance is more specific than risk appetite.**

190- In the context of risk acceptance, choosing not to apply certain controls or safeguards for a specific risk is called:

- Exception (Your answer)
- Evasion
- Exemption (Missed)
- Exclusion

• **Exemption (Correct Answer)** – This refers to a formal decision to waive or not apply certain security controls or safeguards for a specific risk. Exemptions are often documented and approved by management with justification.

• **Exception (Your Answer – Incorrect)** – While similar, an **exception** is typically a temporary deviation from security policies or standards, often requiring approval and a plan for remediation.

191- In the risk acceptance strategy, the practice of temporarily not complying with a standard or policy due to a specific risk scenario is referred to as:

- Exclusion
- Exception (Missed)
- Evasion (Your answer)
- Exemption

192- Which of the following answers refers to a contractual provision that grants one party the right to inspect the other party's operations, facilities, processes, and records?

- Right-to-audit clause (Missed)
- Oversight clause
- Compliance verification clause (Your answer)
- Transparency clause

Right-to-audit clause – This is a contractual provision that grants one party (e.g., a client or regulator) the right to inspect and review the other party's **operations, facilities, processes, and records** to ensure compliance with the agreement, industry standards, or regulations.

Compliance verification clause: While this may require a party to prove compliance, it does not necessarily grant audit rights. Compliance verification can be done through reports, certifications, or third-party assessments rather than direct inspections.

193- In the context of third-party risk assessment and management, which process involves conducting thorough investigations to verify the credentials, reliability, and integrity of potential vendors?

- Reference check
- Compliance review
- Due diligence (Missed)
- Vendor appraisal (Your answer)

Due diligence (Correct Answer) – This is the comprehensive process of **investigating and verifying** a vendor's **credentials, reliability, integrity, security posture, and compliance** before entering a business relationship. It often includes financial, legal, and security assessments.

Vendor appraisal (Your Answer – Incorrect) – While this may involve evaluating a vendor's performance or capabilities, it is generally less comprehensive than due diligence and may not include deep security or integrity checks.

194- Which of the following terms refers to an agreement that specifies performance requirements for a vendor?

- MSA (Your answer)
- SLA (Missed)
- MOU – Memorandum of Understanding
- SOW – Statement of Work

- **SLA (Service Level Agreement) – Correct Answer**

This is a formal contract that defines the **performance requirements** for a vendor, including uptime guarantees, response times, and service quality expectations. SLAs help ensure accountability and set clear expectations.

- **MSA (Master Services Agreement) – Your Answer (Incorrect)**

An **MSA** is a broader contract that defines the overall terms and conditions of a business relationship, but it does not specify detailed performance requirements like an SLA does.

195- Which of the acronyms listed below refers to a formal and often legally binding document that outlines specific responsibilities, roles, and terms agreed upon by two or more parties?

- SOW
- MOA (Missed)
- MSA
- MOU

MOA (Memorandum of Agreement): is a **formal and often legally binding** document that outlines the **specific responsibilities, roles, and terms** agreed upon by two or more parties. It typically goes beyond an **MOU** by defining legally enforceable obligations.

196- A type of nonbinding agreement outlining mutual goals and the general framework for cooperation between two or more parties is referred to as:

- MOA
- SOW
- MOU (Missed)
- MSA

197- Which of the following acronyms refers to a document that authorizes, initiates, and tracks the progress and completion of a particular job or task?

- SOW (Your answer)
- WO (Missed)
- SLA
- MSA

- A **Work Order** is a document that **authorizes, initiates, and tracks** the progress and completion of a specific job or task. It is commonly used in industries like maintenance, construction, and IT services to assign work and track performance.

198- A detailed agreement between a client and a vendor that describes the work to be performed on a project is called:

- MSA
- SLA (Your answer)
- WO
- SOW (Missed)

SOW (Statement of Work): is a detailed agreement that outlines the **specific work to be performed** on a project, including deliverables, timelines, scope, and other critical project details. It serves as a foundation for managing and executing the project.

199- Which of the terms listed below refers to a formal contract between business partners outlining the rights, responsibilities, and obligations of each partner regarding the management, operation, and decision-making processes within the business?

- MSA (Your answer)
- SLA
- BPA (Missed)
- MOA

A **Business Partnership Agreement** is a formal contract that outlines the **rights, responsibilities, and obligations** of each partner involved in a business, including management, operations, and decision-making processes. It ensures that all partners are aligned on how the business will be run.

200- Which of the terms listed below is used to describe actions taken to address and mitigate already identified risks?

- Due diligence
- Standard of care (Your answer)
- Due care (Missed)
- Fiduciary duty

Due care refers to the actions taken to **address and mitigate already identified risks**. It involves the appropriate steps to reduce or eliminate risks after they have been identified, ensuring that reasonable precautions are in place to protect stakeholders and assets.

201- Under data privacy regulations, the individual whose personal data undergoes collection and processing is known as:

- Data holder
- Data owner (Your answer)
- Data user
- Data subject (Missed)

• A **data subject** refers to the **individual** whose **personal data** is collected, processed, or stored. Data privacy regulations, such as GDPR, define rights for the data subject regarding their data, including the right to access, correct, and delete their personal information.

• **Data owner** is typically the entity or individual who has legal ownership or control over the data but is not the individual whose data is being processed

202- Which of the following answers refers to an entity (such as an organization or individual) that determines the purpose and means of processing personal data?

- Data processor (Your answer)
- Data owner
- Data controller (Missed)
- Data subject

• The **data controller** is the entity (such as an organization or individual) that **determines the purpose and means of processing personal data**. They are responsible for ensuring that data processing is done in compliance with applicable laws and regulations (e.g., GDPR).

• **Data processor:** processes personal data on behalf of the data controller, but they do not determine the purpose or means of processing. Their role is more operational, and they act under the instructions of the data controller.

203- An entity that acts under the instructions of a controller by processing personal data on behalf of the controller is called:

- Data steward (Your answer)
- Data processor (Missed)

- Data subject
- Data custodian

A **data steward** is responsible for managing and maintaining data, ensuring its quality and integrity. While they may be involved in overseeing the use of data, they are not directly involved in processing personal data on behalf of a data controller.

204- In cybersecurity exercises, a purple team assumes the integrated role of all other teams (i.e., red, blue, and white).

- True (Your answer)
- False (Missed)

A **purple team** in cybersecurity does not assume the integrated role of all other teams (red, blue, and white). Instead, it facilitates collaboration between the **red team** (offensive, attacking role) and the **blue team** (defensive, protective role). The purple team helps improve the effectiveness of both teams by enhancing communication, knowledge sharing, and coordinated efforts during exercises.

205- In penetration testing, active reconnaissance involves gathering any type of publicly available information that can be used later for exploiting vulnerabilities found in the targeted system.

- True (Your answer)
- False (Missed)

Active reconnaissance involves actively engaging with the target system, such as scanning, probing, or interacting directly with the network or services to gather information about vulnerabilities. This is typically more intrusive and can be detected by the target system.

206- In penetration testing, passive reconnaissance relies on gathering information on the targeted system with the use of various non-invasive software tools and techniques, such as pinging, port scanning, or OS fingerprinting.

- True (Your answer)
- False (Missed)

Passive reconnaissance involves gathering information **without directly interacting** with the target system in a way that could be detected. It relies on publicly available information, such as domain registration details, social media, or other public data sources. It does not involve activities like pinging, port scanning, or OS fingerprinting, as these actions are more intrusive and can be detected.

207- Due to added functionality in its plug, a malicious USB cable can be used for:

- GPS tracking
- Capturing keystrokes (Your answer)
- Sending and receiving commands
- Delivering and executing malware
- Any of the above (Missed)

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

- A worm is propagating across the network
- Data is being exfiltrated
- A logic bomb is deleting data
- Ransomware is encrypting files

High volume of DNS traffic in a nonworking hour is a clear signal of data exfiltration via DNS tunnelling. Attackers usually use dns queries to exfiltrate data outbound the networks.

209- A security pratictioner completes a vulnerability assestments on a company's network and finds several vulnerabilities, wich the operations team remediates. Which of the following should be done next?

- Conduct an audit
- Initiate a Penetration test
- Rescan the network
- Submit a report

After vulnerabilities are found and remediated, the **next step** is to **rescan the network** to verify that: The vulnerabilities have indeed been fixed & No new vulnerabilities have been introduced during remediation.

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

- Secured zones
- Subject role
- Adaptive identity
- Threat scope reduction

"Threat scope reduction" refers directly to the data plane's ability to: limit the impact of attacks, isolate risks, dynamically segment flows, apply granular controls along the data path.
This is precisely what is evaluated in the data plane of a Zero Trust architecture.

211- Which of he following are cases in which an engineer should recommend the decommissioning of a network device? (select two)

- The device has been moved from a production environment to a test environment
- The device is configured to use cleartext passwords
- The device is moved to an isolate segment on the enterprise network
- The device is moved to a different location in the enterprise
- The device's encryption level cannot meet organizational standards
- The device is unable to receive authorized updates

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

- Fines
- Audit findings
- Sanctions
- Reputational damage

This is the **direct outcome** of an internal compliance assessment. The findings identify where the organization fails to meet PCI DSS requirements and guide remediation actions.

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

- Insider threat
- Email phishing
- Social engineering
- Executive whaling

That's a **classic case of social engineering** — using deception or psychological manipulation to trick someone into giving up confidential data or performing an action.

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

- Preparation
- Recovery
- Lesson learned
- Analysis

In the **incident response (IR) process**, the **Preparation** phase is when the organization:

- Defines **roles and responsibilities** of the incident response team.
- Establishes **policies, procedures, and communication plans**.
- Ensures tools and resources are in place before an incident occurs.

215- After reviewing the following vulnerability scanning report:
Server: 192.168.14.6 – Service: Telnet – Port: 23 – Protocol TCP – Satus Open – Severity: High Vulnerability: Use of an insecure network protocol
A security analyst performs the following test: nmap -p 23 192.168.14.6 - script telnet-encryption PORT STATE SERVICE REASON 23/tcp open telent syn-ack I telent encryption: | _ Telent server support encryption.
Which of the following would the security analyst conclude for this reported vulnerability?

- It is a false positive
- A rescan is required
- It is considered noise
- Compensating control exist

This output shows that **the Telnet server supports encryption**, meaning it is **not transmitting data in cleartext**, which **mitigates the vulnerability**.

Therefore:

- The scanner's report identified Telnet as insecure by default (which is often true).
- Manual validation proved encryption **is enabled**.
- This means the reported vulnerability is **not actually present**.

👉 **Conclusion: It is a false positive.**

216- A chief information security officer (CISO) wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigation if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

- Logging all network traffic into a SIEM
- Deploying network traffic sensors on the same subnet as the servers
- Logging endpoint and OS-Specific security logs
- Enabling full packet capture for traffic entering and exiting the servers

SQL injection payloads live in the application-layer traffic (HTTP requests). With SSL decryption in place, full packet capture (PCAP) records the complete, reassemble-able network conversation — including the exact HTTP requests, query parameters, and responses — which is essential for confirming an SQLi, reconstructing the attack timeline, and performing a comprehensive forensic investigation.

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

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

When a new vulnerability is disclosed, a security analyst must quickly determine **which systems are affected**. To do that accurately, the analyst needs a **comprehensive inventory** of all hardware and software assets within the organization.

218- 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?

- Insurance
- Patching
- Segmentation
- Replacing

Because the vulnerability affects **legacy IoT devices**, patching may not be immediately possible (or even available), and replacing all devices would take time and resources. Therefore, the **quickest and most effective mitigation** is to **segment** those vulnerable devices from the rest of the network.

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

- Concurrent session usage
- Secure DNS cryptographic downgrade
- On-path resource consumption
- Reflected denial of service

The **DNS server** is being flooded with **inbound network traffic**, but:

  - **CPU, disk, and memory usage are low** → meaning it's not processing many legitimate queries.
  - **Logs show only a small number of DNS queries** → indicating the traffic isn't legitimate DNS requests from users.

This pattern fits a **reflected DDoS attack**, where attackers use **open DNS resolvers** to reflect and amplify traffic toward a victim. In this case, the DNS server is likely being used as part of a **reflection/amplification attack** — attackers send small queries with a **spoofed source IP (the**

victim's address), and the DNS server replies with large responses to the victim, flooding it with data.

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

a. RBAC
b. ACL
c. SAML
d. GPO

RBAC allows permissions to be assigned based on users' roles and responsibilities. It provides a **simplified, structured way** to manage access by grouping users into roles instead of assigning individual permissions one by one. This makes it ideal for controlling access to sensitive resources — such as a **site recovery resource group** — based on job function.

221- A company has begun labelling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do the 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

✅ **a. Incident ownership:** If a laptop generates suspicious activity or is involved in a security incident, the security team can quickly identify **which employee is responsible** for the device and contact them.

✅ **f. Asset accountability:** When an employee leaves the organization, asset tracking ensures all company equipment is returned. It also helps make sure that **company data stored on that device is secured or wiped**.

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

a. Remote access points should fail close
b. Logging controls should fail open
c. Safety controls should fail open
d. Logical security controls should fail closed

When reviewing controls in a data center, two major priorities must be considered:

1. **Protection of data and systems**
2. **Protection of human life**

In safety-critical situations, **human life always takes precedence over security.**
Therefore, **safety controls must fail open**—meaning if the system fails, doors unlock and people can evacuate safely.

223- A business received a samll grant to migrate it's infrastructure to an off-premises solution. Which of the following ahould be considered frist?

a. Security of cloud providers
b. Cost of implementation
c. Ability of engineers
d. Security of architecture

Before migrating infrastructure off-premises, the **first** and most critical consideration is the **security posture of the cloud providers** you are evaluating. This includes:

- Compliance certifications
- Data protection mechanisms
- Identity and access controls
- Physical and logical security
- Incident response capabilities

224- 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

A **bastion host** is a hardened, publicly accessible system used to provide secure administrative access to internal resources. It minimizes the amount of traffic passing through the security boundary by acting as a **single, controlled entry point** for administrators.

Key benefits: Centralized access point, Strong authentication controls, Reduced attack surface, Monitoring and logging of admin access

225- A security analyst review domain activity logs and notices the following:

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

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

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

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

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

a. the user jsmith's account has been locked out
b. a keylogger is installed on smith's workstation
c. an attacker is attempting to brute force jsmith's account
d. ransomware has been deployed in the domain

The logs show **multiple successful password authentications** but **repeated MFA failures**. This strongly indicates the attacker already knows or has compromised the user's password but is failing the second factor (MFA code).

This is a typical pattern when:

- Password is stolen (phishing, credential stuffing, breach reuse).
- Attacker attempts to guess or brute-force the MFA code.
- They repeatedly try logging in but cannot pass MFA.

Why not the others?

- **a. The account has been locked out**
  If it were locked out, authentication attempts would fail, not succeed.
- **b. A keylogger is installed**
  A keylogger would give the attacker both the password and the MFA code only if the user types it — but the attacker is failing MFA.
- **d. Ransomware has been deployed**
  This log pattern does not indicate ransomware activity.

226- Which of the following security concepts is the best reason for permission on a human resources file share to follow the principle of least privilege?

a. Integrity
b. Availability
c. Confidentiality
d. Non-repudation

The **principle of least privilege** ensures users only have access to the information necessary to perform their job duties. Restricting access helps maintain **confidentiality**, preventing unauthorized disclosure of sensitive data.

227- Several employees received a fraudulent text message from someone caliming to be the 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. Issuing a general email warning to the company
d. Have the CEO changed phone numbers
e. Conduct a forensic investigation on the CEO’s phone
f. Implement MDM (mobile device management)

This scenario is a classic **smishing** attack (SMS phishing) impersonating an executive to trick employees into buying gift cards — a common social engineering tactic.

✅ **b. Add a smishing exercise to the annual company training**

This strengthens future employee awareness by teaching staff to recognize fraudulent SMS messages.
Training is a key defense against social engineering.

✅ **c. Issuing a general email warning to the company**

This helps notify all employees quickly about the scam and prevents others from falling for it.
It also reinforces awareness that executives usually do not make such requests.

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

a. Retain the emails between the security team and affected customers for 30 days
b. Retain any communications related to the security breach until further notice
c. Retain any communications between security members during the breach response
d. Retain all emails from the company to affected customers for an indefinite period of time

A **legal hold** (also called litigation hold) is a directive from legal counsel that requires the preservation of all records and data that may be relevant to ongoing or anticipated litigation. This means:

- All communications **related to the breach** must be preserved.
- The hold lasts **until legal counsel releases it** — not a fixed number of days.
- It includes all formats: emails, chat logs, documents, reports, etc.

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

a. Default credentials
b. Non-segmented network
c. Supply chain vendor
d. Vulnerable software

Since the system is **supported by a SaaS provider**, the organization is relying on an external third party for critical services. This introduces **supply chain risk**, because:

- The organization does not fully control the software.
- Any compromise of the SaaS provider could impact the organization.
- Opening ports increases exposure to potential third-party security weaknesses.

230- An admin is reviewing a single server's security logs and discovers the following

Audit failure 09/16/2022 11:13:05am Microsoft Windows security 4625 Logon

Audit failure 09/16/2022 11:13:07am Microsoft Windows security 4625 Logon

Audit failure 09/16/2022 11:13:09am Microsoft Windows security 4625 Logon

Audit failure 09/16/2022 11:13:11am Microsoft Windows security 4625 Logon

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

a. Brute-force attack
b. Privilege escalation
c. Failed password audit
d. Forgotten password by the user

The log shows **many repeated logon failures** (Event ID 4625) within very short time intervals. The failures are occurring one after another, indicating **multiple attempts in rapid succession**. This pattern is **characteristic of a brute-force attack**, where an attacker or automated script repeatedly tries different passwords to gain access.

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

a. SPF
b. GPO
c. NAC
d. FIM

File integrity monitor: **FIM** is designed specifically to **detect and track changes to files**, configurations, or system data. It monitors critical system files and alerts administrators if anything is modified, added, or deleted, making it ideal for ensuring data integrity and tracking changes.

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

a. Hashing
b. Tokenization
c. Encryption
d. Segmentation

To ensure sensitive **data at rest** is **unreadable** without proper authorization, the company will use **encryption**. Encryption converts data into ciphertext, which cannot be interpreted without the correct decryption key.

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

a. Console access
b. Routing protocols
c. VLANs
d. Web-based administrator

When hardening routers, the goal is to **reduce the attack surface**. The **web-based administrative interface** (HTTP/HTTPS management GUI) is often one of the **most targeted and vulnerable** features because:

- It exposes a management interface over the network
- It can be brute-forced or exploited remotely
- GUI management interfaces historically have more vulnerabilities than CLI access

Therefore, disabling **web-based administration** is the most appropriate and common hardening step.

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

a. Real time recovery
b. Hot
c. Cold
d. Warm

A cold site is the most cost-effective type of backup data center. It provides basic infrastructure (space, power, cooling) but does not include pre-installed hardware or live data, which makes it inexpensive compared to warm or hot sites.

With RTO and RPO around two days, this aligns perfectly with the characteristics of a cold site:

- Longer recovery time → acceptable (up to days)
- Lower cost → primary requirement
- No immediate operational capability → setup time required

❌ Why the others incorrect:

- a. Real-time recovery → Implies near-zero downtime and continuous replication (very expensive).
- b. Hot → Fully operational, minimal downtime (minutes to hours). Too expensive.
- d. Warm → Partially equipped, recovery within hours, not days. Higher cost than cold.

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

a. Private
b. Confidential
c. Public
d. Operational
e. Urgent
f. Restricted

For a critical government system, the information stored on a file share would most likely be classified as:

✅ Confidential — Government project data is not meant for public access and requires controlled access.

✅ Restricted — Access would be limited only to authorized personnel due to the sensitivity of the system.

236- Which of the following would be the best way to block unknow programs from executing?

a. Access control list
b. Application allow list
c. Host-based firewall
d. DLP solution

Application allow list (whitelisting): This approach only allows approved programs to run on a system. Any program **not explicitly allowed** is blocked automatically. This is the **most effective way to prevent unknown or unauthorized programs from executing**.

237- A system admin works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classification should be used to secure patient data?

a. Private
b. Critical
c. Sensitive
d. Public

Sensitive data refers to information that must be protected due to privacy or regulatory requirements. **Patient data (PHI – Protected Health Information)** falls under this category because unauthorized disclosure could violate privacy laws (like HIPAA in the U.S.) and harm patients

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

a. A thorough analysis of the supply chain
b. A legally enforceable corporate acquisition policy
c. A right to audit clause in vendor contracts and SOW's
d. An in-depth penetration testing of all suppliers and vendors

Counterfeit hardware often enters networks through insecure or unreliable supply chains. By performing a **thorough supply chain analysis**, the company can verify the authenticity, origin, and certification of hardware before procurement, reducing the risk of counterfeit components.

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

a. Encryption
b. Hashing
c. Masking
d. Tokenization

Masking hides most of the PAN and shows only the last four digits (e.g., **********1234), which exactly meets the requirement.

- **Encryption** protects data at rest/in transit but still allows full recovery (not just last-4).
- **Hashing** is one-way — you can't recover digits to display the last four.
- **Tokenization** replaces the PAN with a token (useful for processing) but doesn't by itself imply showing only the last four; masking is the direct method for that display requirement.

240- 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

When designing a **high-availability (HA)** network, the primary goals are to ensure services remain accessible with minimal downtime and to restore full functionality quickly in case of failures.

241- A company's accounts payable clerk receives an email from a vendor asking to change their bank account information. After updating it, the payment is sent. Days later, the real vendor asks why payment was not received. What occurred?

a. Phishing campaign
b. Data exfiltration
c. Pretext calling
d. Business email compromise

Explanation: An attacker impersonated the vendor to redirect payments.

242- What process should HR follow to track revisions after multiple document iterations?

a. Version retention
b. Version changes
c. Version updates
d. Version control

Explanation: Version control tracks changes and document history.

243- A RADIUS server implements which security concept?

a. CIA
b. AAA
c. ACL
d. PEM

Explanation: RADIUS provides authentication, authorization, and accounting.

244- Employees report blocked pages warning of spoofed websites. What should be done?

a. Deploy MFA
b. Lower web filter level
c. Implement security awareness training
d. Update acceptable use policy

Explanation: Training helps employees identify phishing attempts.

245- Difference between hashing and encryption?

a. Encryption for transit, hashing for rest
b. Encryption creates ciphertext, hashing creates checksum
c. Hashing provides confidentiality
d. Hashing uses private keys

Explanation: Hashing is one-way; encryption is reversible.

246- SIEM shows same user logging in from many countries within minutes. What is happening?

a. Brute force
b. Privilege escalation
c. XSS
d. Password sharing

Explanation: Impossible logins indicate credential sharing.

247- Which log to review to find SQL injection commands?

a. Metadata
b. Application log
c. System log
d. Netflow log

Explanation: Application logs contain executed SQL queries.

248- A school admin wants to block inappropriate sites. Which tool helps?

a. Reputation filters
b. NAC
c. UBA
d. Content categorization

Explanation: Categorization blocks sites by content type.

249- Data moved from production to UAT. How to protect?

a. Masking
b. Tokenization
c. Obfuscation
d. Encryption

Explanation: Masking ensures sensitive data is anonymized for testing.

250- EDR belongs to which control category?

a. Physical
b. Operational
c. Managerial
d. Technical

Explanation: EDR is a technical control.

251- Why ensure multiple team members understand an automation script?

a. Reduce cost
b. Identify complexity
c. Remediate technical debt
d. Avoid single point of failure

Explanation: Knowledge redundancy prevents dependency

252- Why are environment variables a vulnerability concern?

a. Contents affect impact of exploited vulnerability
b. Variables are overwritten to insert code
c. They define crypto standards
d. They schedule updates

Explanation: Sensitive env vars increase impact if compromised.

253- Best method to protect data on decommissioned laptops?

a. Wiping
b. Recycling
c. Shredding
d. Deletion

Explanation: Wiping securely removes data cheaply.

254- Inspecting new servers for motherboard tampering mitigates which risk?

a. Embedded rootkit
b. Supply chain
c. Firmware failure
d. RFID keylogger

Explanation: Visual inspection detects supply chain tampering.

255- Prevent data leakage on a network not needing external communication?

a. Air gap
b. Containerization
c. Virtualization
d. Decentralization

Explanation: Air-gapping fully isolates the network

256- Requesting SOC 2 from SaaS vendor is part of?

a. Internal audit
b. Penetration test
c. Attestation
d. Due diligence

Explanation: Evaluating vendor risk.

257- Direct consequence of non-compliance with privacy law?

a. Fines
b. Reputation damage
c. Sanctions
d. Contract implications

Explanation: Legal penalties occur first.

258- University using two cloud providers demonstrates?

a. Load balancing
b. Parallel processing
c. Platform diversity
d. Clustering

Explanation: Multiple cloud platforms.

259- Training employees after phishing credential leak reduces?

a. Outbound blocking
b. Failure-based restrictions
c. Phishing susceptibility
d. Web deny-list reliance

Explanation: Awareness reduces credential theft.

260- Which provides control assurances?

a. Red team
b. Pen test
c. Independent audit
d. Vulnerability scan

Explanation: Third-party audits validate control effectiveness.

261- New regulation upcoming — what next?

a. Gap analysis
b. Policy review
c. Procedure evaluation
d. Threat reduction

Explanation: Identify compliance gaps first.

262- Rogue Wi-Fi devices reconnect after passkey change. Cause?

a. Brute force
b. Trojan
c. Replay attack
d. Keylogger

Explanation: Keylogger captured new password.

263- Protect data integrity and confidentiality?

a. Obfuscation
b. Tokenization
c. Digital certificate
d. Masking

Explanation: Certificates provide encryption + signing

264- Best quarantine action?

a. Air-gap device
b. Disable remote login
c. Convert to sandbox
d. Remote wipe

Explanation: Isolation prevents spread.

265- Restrict uploads but allow downloads?

a. IDS
b. IPS
c. WAF
d. NGFW

Explanation: NGFW supports directional filtering.

266- SaaS deployment risk when opening firewall ports?

a. Default credentials
b. Network segmentation
c. Supply chain vendor risk
d. Vulnerable software

When deploying a **SaaS application**, the company is relying on an **external third-party provider** for:

- hosting
- data storage
- application security
- patching
- availability