Security+ 701 مكثف التنين

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Note: These notes summarize key Security+ concepts and are meant to support, not replace, comprehensive study of the official CompTIA materials.

Category	Description
Something you know but important	important ,read
Important	Important, Focus on it
Examples	Examples, e.g.
Ignore	Ignore
Read	Read

START

- 2 Questions | Lesson 1: Fundamental Security Concepts
- 9 Questions | Lesson 2: Threat Types
- 6 Questions | Lesson 3: Cryptographic Solutions
- 3 Questions | Lesson 4: Identity and Access Management (IAM)
- 5 Questions | Lesson 5: Enterprise Network Architecture
- 3 Questions | Lesson 6: Cloud & Zero Trust
- 6 Questions | Lesson 7: Resiliency and Site Security
- 5 Questions | Lesson 8: Vulnerability Management
- 4 Questions | Lesson 9: Network Security Capabilities
- 4 Questions | Lesson 10: Endpoint Security
- 1 Questions | Lesson 11: Application Security
- 9 Questions | Lesson 12: Alerting and Monitoring
- 3 Questions | Lesson 13: Analyze Indicators of Malicious Activity
- 10 Questions | Lesson 14: Security Governance Concepts
- 8 Questions | Lesson 15: Risk Management Processes
- 8 Questions | Lesson 16: Data Protection and Compliance Concepts

Lesson	Title	Questions	Weight (%)
1	Fundamental Security Concepts	2	**2.08%**

2	Threat Types	9	**9.38%**
3	Cryptographic Solutions	6	**6.25%**
4	Identity and Access Management (IAM)	3	**3.13%**
5	Enterprise Network Architecture	5	**5.21%**
6	Cloud & Zero Trust	3	**3.13%**
7	Resiliency and Site Security	6	**6.25%**
8	Vulnerability Management	5	**5.21%**
9	Network Security Capabilities	4	**4.17%**
10	Endpoint Security	4	**4.17%**
11	Application Security	1	**1.04%**
12	Alerting and Monitoring	9	**9.38%**
13	Analyze Indicators of Malicious Activity	3	**3.13%**
14	Security Governance Concepts	10	**10.42%**
15	Risk Management Processes	8	**8.33%**
16	Data Protection and Compliance Concepts	8	**8.33%**

Lesson 1: Fundamental Security Concepts

1. **CIA Triad**
   - **Confidentiality, Integrity, Availability** (Core security principles).
   - **Non-repudiation** (Proof of origin/actions).
2. **Cybersecurity Frameworks**
   - **NIST Cybersecurity Framework (CSF)** (Identify, Protect, Detect, Respond, Recover).
   - **Gap Analysis** (Comparing current vs. desired security posture).

     Frameworks provide structured approaches to managing cybersecurity risks.
     - **NIST Cybersecurity Framework (CSF)**:
       - A U.S. government guideline for improving cybersecurity.
       - **5 Core Functions**:
         1. **Identify** (asset management, risk assessment).
         2. **Protect** (access control, encryption).
         3. **Detect** (monitoring, anomaly detection).
         4. **Respond** (incident response plan).
         5. **Recover** (backups, continuity planning).

Function	Description with Examples (Naturally Embedded)
Identify	This phase is all about understanding what needs protection. If you hear terms like asset inventories, risk evaluations, or classifying systems based on business impact, it's tied to this function. Think of

	mapping out users, devices, data, and identifying where vulnerabilities or critical assets exist.
Protect	Measures taken here aim to secure systems before an incident happens. If you come across encryption protocols, MFA (multi-factor authentication), user training programs, or hardening configurations, you're seeing efforts to safeguard against threats. This includes limiting access, securing endpoints, and enforcing security policies.
Detect	When systems are actively looking for suspicious behavior or unexpected changes, you're in the detection phase. This includes log analysis, IDS/IPS, SIEM tools, or receiving alerts from monitoring tools when something deviates from the norm. Anomalous login attempts or strange network spikes? Detection in action.
Respond	Once an incident occurs, this phase kicks in. You might hear about isolating systems, notifying stakeholders, activating an incident response playbook, or forensics investigation. Anything involving mitigation steps, coordination with teams, or containment efforts belongs here.
Recover	The focus here is getting back to normal operations. If you see references to restoring from backups, disaster recovery sites, continuity of operations plans, or lessons learned meetings after a breach, it's part of recovery. It's about resilience and minimizing downtime.

- **ISO 27001 & ISO 27002**:
  - **ISO 27001**: Establishes requirements for an **Information Security Management System (ISMS),used for international best practices too** .
  - **ISO 27002**: Provides best practices for security controls (encryption, access control).
- **Gap Analysis**:
  - Compares an organization's current security measures against a standard (NIST, ISO).
  - Helps identify weaknesses and compliance gaps.

1. **Access Control Models**
   - **AAA Framework** (Authentication, Authorization, Accounting).
     - **AAA Framework**:
       - **Authentication**: Verifies identity (passwords, MFA, biometrics).
       - **Authorization**: Determines permissions (RBAC, ABAC).
       - **Accounting**: Logs actions (audit trails, SIEM).

Component	What It Does	Examples / Technologies
Authentication	Verifies identity	**RADIUS**, **TACACS+**, LDAP, Kerberos, biometrics (fingerprint scanner), smart cards, password-based login, MFA apps (like Google Authenticator)
Authorization	Determines what a user can access	Role-based permissions (**RBAC systems**), group policies in Active Directory, firewall rules per user, access control lists (ACLs), ABAC engines
Accounting	Tracks user activity	**RADIUS accounting**, **TACACS+ logs**, **Syslog**, **SIEM systems** (like Splunk or QRadar), audit trails, login history, file access logs

- **Access Control Models**:
  - **RBAC (Role-Based)**: Permissions based on job role.
  - **MAC (Mandatory)**: Labels (Top Secret, Confidential).
  - **ABAC (Attribute-Based)**: Dynamic rules (time, location).
  - **DAC (Discretionary)**: Owner-controlled (file permissions).

Model	Description
RBAC	This model organizes permissions based on organizational roles. A user's access is determined by their assigned position, simplifying management by grouping users with similar duties. You'll often see references to roles, hierarchy, and job functions.
MAC	Access decisions are tightly enforced through policies set by a central authority. Information is tagged with classification levels, and users must have appropriate clearance. Mentions of labels, clearance levels, and strict control usually point to this.
ABAC	Access is granted through evaluating multiple attributes related to the user, resource, and environment. Decisions adapt based on dynamic conditions. Look for hints like policies considering time, device, location, or user profile.
DAC	Here, the control lies with the individual owner of the resource. Users can decide who else can access their objects. If ownership, sharing rights, or user-defined access rules are mentioned, this model is likely in use.
Rule-Based Access Control	Access is regulated through predefined rules that apply universally, often outside the context of user roles. The focus is on system-wide conditions and logic, so when you see conditions like "all users must..." or centralized rule sets, this model is implied.

2. **Security Control Types**
   - **Managerial, Operational, Technical, Physical** (Categories).
   - **Preventive, Detective, Corrective, Deterrent, Compensating** (Functional types).
     - **By Category**:
       - **Technical**: Firewalls, IDS/IPS, encryption.
       - **Managerial**: Define security strategy and manage risk at a policy level. ex: Security policies, risk assessments, compliance requirements, audit planning
       - **Operational**: Execute and enforce policies through day-to-day procedures, ex: Security awareness training, incident response plans, backup operations, physical security
       - **Physical**: Locks, cameras, biometric scanners.
     - **By Function**:
       - **Preventive**: Firewalls, encryption.
       - **Detective**: IDS, CCTV, log monitoring.
       - **Corrective**: Patches, backups, incident response.
       - **Deterrent**: Warning signs, fines.
       - **Compensating**: Alternative controls (MFA if passwords are weak).
       - **Directive**: Security awareness training, incident response plan, onboarding policies.

Category	Function	Examples (Realistic & Recognizable)
Technical	Preventive	Firewalls blocking unauthorized ports, encryption for data-in-transit, antivirus software
	Detective	Intrusion Detection Systems (IDS), SIEM alerts, security logs reviewed for anomalies
	Corrective	Security patches for vulnerabilities, system restore from backup after malware
Managerial	Preventive	Written security policies (acceptable use), risk assessments to avoid threats, mandatory training plans
	Detective	Audit reports revealing policy violations, compliance checks by internal audit teams
	Corrective	Updating policy after a breach, enforcing new guidelines post-incident
Operational	Preventive	Scheduled backups, change control procedures, disaster recovery drills
	Detective	Security awareness testing (phishing simulations), log reviews by staff
	Corrective	Activating incident response plan, restoring data from offline backups
Physical	Preventive	Door locks, ID badges, mantraps, biometric access control (fingerprint scanners)
	Detective	CCTV surveillance recording intrusions, motion sensors triggering alerts
	Corrective	Replacing broken locks, repairing security gates after tampering
	Deterrent	“Area under surveillance” signs, visible security guards, alarm systems
	Compensating	Locked server cage when door access control is broken, requiring two guards for access instead of biometrics

Function Type	Extra Examples
Preventive	Network segmentation, MFA, screen filters, secure coding practices
Detective	File integrity monitoring, honey pots, data loss detection systems
Corrective	Re-imaging infected machines, applying hotfixes, changing compromised passwords
Deterrent	Disciplinary policies, warning banners, visible audit trails
Compensating	MFA in place of outdated password policy, security guard when access system is offline
Directive	Security awareness training, policies and procedures, onboarding manuals

---

3. **Information Security Roles and Responsibilities**

- **Chief Information Officer (CIO):Overall responsibility for the IT function**
- **Chief Technology Officer (CTO): making effective use of new and emerging computing platforms**
- **Development and operations (DevOps):A combination of software development and systems operations**
- **DevSecOps:A combination of software development, security operations, and systems operations**
- **computer incident response team (CIRT):Team with responsibility for incident response**
- Security operation center (SOC):security professionals monitor and protect critical information assets in an organization.
- **Chief Security Officer (CSO):overall responsibility for information assurance and systems security**

Information Systems Security Officer (ISSO): technical responsibilities for implementation of security policies, frameworks, and controls

---

Lesson 2: Threat Types

1. Threat Actors and Attributes

Core Concepts

- **Vulnerability vs. Threat vs. Risk**:
  - **Vulnerability**: Weakness in a system (unpatched software).
  - **Threat**: Potential danger (hacker exploiting the vulnerability).
  - **Risk**: Impact × Likelihood of the threat occurring.

Threat Actor Attributes

Attribute	Description
Internal/External	Internal: Authorized users (employees). External: Outsiders.
Sophistication	Low (script kiddies) vs. High (nation-states).
Resources	Organized crime (funded) vs. hacktivists (ideological).

Motivations

Type	Examples
Financial	Ransomware, fraud.
Political	Espionage (APT groups).
Chaotic	Hacktivists (Anonymous).
Accidental	Insider mistakes.

Key Threat Actor Types

- **Hacktivists.**
- **Nation-State Actors**: APTs (APT29).
- **Organized Crime**: Profit-driven (ransomware gangs).
- **Insiders**: Malicious (sabotage) or negligent (shadow IT).

Threat Actor Type	Motivation	Common Tactics
Hacktivists	- Political/social change	- DDoS attacks
	- Ideological beliefs	- Website defacement
	- Public shaming	- Data leaks
Nation-State Actors	- Espionage	- Zero-day exploits
	- Political disruption	- Advanced persistent threats (APTs)
	- Cyber warfare	- Supply chain attacks
Organized Crime	- Financial gain	- Ransomware

Threat Actor Type	Motivation	Common Tactics
	- Extortion	- Phishing campaigns
		- Cryptojacking
Insiders	- Revenge (malicious)	- Data theft
	- Financial gain	- Sabotage
	- Accidental negligence	- Unintentional breaches

Hacktivists are ideologically motivated attackers who target organizations to promote political or social causes. They use disruptive tactics like DDoS attacks, website defacements, and data leaks to embarrass their targets and draw public attention to their agenda. Their operations are typically low-budget, relying on volunteer efforts and publicly available tools, and they often claim responsibility to amplify their message. Examples include groups like Anonymous.

Nation-State Actors are government-sponsored hackers who conduct cyber operations for espionage, sabotage, or political influence. They employ advanced, stealthy techniques like zero-day exploits, long-term APTs (Advanced Persistent Threats), and supply chain attacks to infiltrate critical infrastructure, military systems, or corporate secrets. Unlike hacktivists, they avoid attribution, operate with significant funding, and prioritize long-term access over publicity. Examples include groups like APT29 (Russian Cozy Bear) and APT41 (China).

Key SEC+ Focus:

- Hacktivists = disruptive, public, ideological.
- Nation-States = stealthy, strategic, well-funded.

---

2. Attack Vectors and Surfaces

Attack Surface Components

Surface	Examples
Physical	Unsecured server rooms.
Network	Open ports, weak credentials.
Human	Social engineering.
Software	Zero-day vulnerabilities.

Common Attack Vectors

1. Network-Based Vectors

- **Exploits**: Targeting vulnerabilities in protocols (Bluetooth, DNS, HTTP).
- **Misconfigurations**: Unsecured cloud storage, open ports, default credentials.
- **MITM Attacks**: Intercepting unencrypted traffic.
- **DoS/DDoS**: Overwhelming systems with traffic.

2. Lure-Based Vectors

- **Malicious USB Drops**: Physical devices with auto-executing malware.
- **Trojanized Software**: Fake downloads (pirated tools).
- **Malicious Documents**: Office files with macros/scripts.
- **Image/PDF Exploits**: Exploiting viewer vulnerabilities.

3. Message-Based Vectors

- **Phishing**: Fraudulent emails (fake login pages).
- **SMiShing/Vishing**: SMS/voice scams ("Your account is locked").
- **Social Media Scams**: Fake profiles, malicious links.

- **Business Email Compromise (BEC)**: Impersonating executives for wire fraud.

4. Supply Chain Vectors

- **Compromised Software Updates**: Malware injected into vendor updates (SolarWinds).
- **Third-Party Access**: Exploiting MSPs/vendors with weak security.
- **Hardware Tampering**: Modified devices pre-delivery.

SEC+ Exam Focus

- **Memorize**:
  - **Network** = Protocol exploits/misconfigurations.
  - **Lure** = Physical/digital bait (USB/docs).
  - **Message** = Phishing/SMiShing/BEC.
  - **Supply Chain** = Vendor compromises.

MITRE ATT&CK Framework

- **Tactics**: Initial access, lateral movement, exfiltration.
- **Techniques**: Spear phishing (T1566), credential dumping (T1003).

---

3. Social Engineering Techniques

Methods

Technique	Description
Phishing	Fake emails ("Reset your password").
Vishing/SMiShing	Voice calls/text scams.
Pretexting	Fabricated scenarios ("IT needs your login").
BEC	CEO fraud ("Wire $1M urgently").

Human Vectors

- **Impersonation**: Posing as IT staff/vendors.
- **Urgency**
- **Authority**
- **Fmiliarity**
- **Consensus**
- **Social proof**

Urgency

- *Definition*: Creating artificial time pressure to bypass rational thinking
- *Attack Patterns*:
  - "Your account will be deleted in 24 hours"
  - "Limited-time offer expires in 30 minutes"
- *Psychology*: Activates fight-or-flight response → hasty actions
- *SEC+ Focus*: Key red flag in phishing emails

Authority

- *Definition*: Exploiting hierarchical obedience tendencies
- *Attack Patterns*:
  - "This is the CEO - transfer funds immediately"
  - "IT Department requires your password"
- *Psychology*: Leverages automatic compliance with perceived superiors

Vector	Key Difference / Description
Impersonation	Attacker pretends to be someone trustworthy (IT, vendor, executive) to gain access or information. Relies on **trust in roles**.
Urgency	Pressures the target to act quickly without thinking (“your account will be locked”). Relies on **stress and time pressure**.
Authority	Exploits the perception of power (posing as a CEO or police). Relies on **compliance with perceived power**.
Familiarity	Uses shared interests, casual tone, or knowledge of personal details to seem trustworthy. Relies on **false rapport or common ground**.
Consensus	Convinces the target that “others have already done this” (everyone already reset their password i need you to reset your password too). Relies on **herd behavior**.
Social Proof	Shows evidence (real or fake) that others trust the attacker or action (fake testimonials or endorsements). Relies on **validation by others' actions**.

Lesson 3: Cryptographic Solutions

1. Encryption Standards

Symmetric Encryption

- **Algorithms**:
  - AES (256-bit) - Gold standard for bulk encryption
  - 3DES (168-bit) - Legacy, being phased out
  - Blowfish/Twofish - Older alternatives
- **Properties**:
  - Same key for encryption/decryption
  - Fast but insecure key distribution
  - Modes: CBC, GCM (with authentication)

Asymmetric Encryption

- **Algorithms**:
  - RSA (2048-bit+) - Key exchange/digital signatures
  - ECC (256-bit+) - Efficient for mobile devices
  - Diffie-Hellman - Key exchange only IKE
- **Properties**:
  - Key pairs (public/private)
  - Slow, used for small data like key exchange

Hashing

- **Algorithms**:
  - SHA-256/512 - Current standard
  - MD5 (128-bit) - Broken, used only for checksums
- **Properties**:
  - One-way function (no decryption)
  - Used for password storage (with salt) and integrity checks

Term	Meaning
Weak Keys	Keys that are easy to guess, short, or not random enough; vulnerable to brute-force attacks.
Strong Keys	Long and random keys that are hard to guess; resist brute-force and dictionary attacks.
Key Stretching	A method to make weak keys stronger by processing them through algorithms like PBKDF2, bcrypt, or scrypt.
Key Exchange	The secure sharing of cryptographic keys between parties (Diffie-Hellman).
Ephemeral Keys	Temporary keys used only for one session, enhancing security (in ECDHE).
Asymmetric Keys	Two-key system (public/private); used in encryption and digital signatures.
Symmetric Keys	One shared key used for both encryption and decryption; faster but needs secure key exchange.
Perfect Forward Secrecy (PFS)	Uses ephemeral keys to ensure past sessions stay secure even if one key is compromised.

1. Encryption (for confidentiality)

Goal: Only Bob can read the message.

When Alice sends a private message **to Bob**:

- **Alice uses Bob's public key** to encrypt the message.
- **Bob uses his private key** to decrypt the message.

Step	Key Used
Alice encrypts	Bob's **public key**
Bob decrypts	Bob's **private key**

---

2. Digital Signature (for integrity + authenticity)

Goal: Bob can be sure **Alice** sent the message and it hasn't been changed.

When Alice signs a message:

- **Alice hashes the message**, then **signs the hash with her private key**.
- **Bob uses Alice's public key** to verify the signature.

Step	Key Used
Alice signs hash	Alice's **private key**
Bob verifies	Alice's **public key**

---

2. PKI & Certificates

Public key infrastructure (PKI) refers to a framework of Certificate Authorities (CAs), digital certificates, software, services, and other cryptographic components deployed to validate subject identities.

X.509 Certificate Components

- **Fields**:
  - Subject (CN, SAN)
  - Issuer (CA)
  - Validity dates
  - Key Usage (Digital Signature, Key Encipherment)
- **Formats**:
  - .pem (Base64), .der (Binary), .pfx/.p12 (with private key)

Certificate Authorities

- **Hierarchy**:
  - Root CA → Intermediate CA → Leaf certificates
- **Trust Models**:
  - Public CA (DigiCert, Let's Encrypt)
  - Private CA (Enterprise PKI)
  - Self-signed (No chain of trust)

Revocation Methods

1. OCSP (Online Certificate Status Protocol)

- **Used to validate certificates** in real-time.
- It checks with the **Certificate Authority (CA)** to see if a cert is **still valid or revoked**.
- When a user receives a certificate (like from a website), OCSP helps say "yes, this cert is good."

---

2. CSR (Certificate Signing Request)

- This is what you send to a CA **when you're requesting a certificate**.
- Containing the information that the subject wants to use in the certificate, including its public key
- Not used for validation at all.

---

3. CA (Certificate Authority)

- This is the entity that **issues** and **manages** certificates.
- The CA provides certs and can revoke them, but **it's OCSP that's used to validate** them dynamically.

---

4. CRC (Cyclic Redundancy Check)

- It's a **checksum method** used for **data integrity**, like checking files or data blocks.
- **Not related to certificate validation.**

5.CRL (certificate revoke list)

- A list of certificates that were revoked before their expiration date.
- A Certificate Authority (CA) or owner can revoke or suspend a certificate for many reasons. A Certificate Revocation List (CRL) is a list of no longer valid certificates.

---

3. Key Management

Key Lifecycle

1. Generation → 2. Distribution → 3. Storage → 4. Rotation → 5. Destruction

Secure Storage

- **HSM**: Tamper-proof hardware for key storage (Key escrow)
- **TPM**: On-board crypto processor for device keys
- **Secure Enclave**: Isolated CPU area (Apple Secure Enclave)

Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes

TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication

Key Exchange Protocols

- **KMIP**: Standard for centralized key management
- **PKCS#7/#12**: Formats for key/cert transfer

---

4. Advanced Concepts

Perfect Forward Secrecy (PFS)

- Ephemeral keys for each session
- Prevents mass decryption if long-term key is compromised
- Used in TLS 1.3

Blockchain

- Decentralized ledger with cryptographic hashing
- Immutable records (Bitcoin, smart contracts)

Obfuscation Techniques

Technique	Use Case
Steganography	Hiding data in images (LSB method)
Tokenization	Replacing sensitive data with tokens (PCI DSS) ex: 0192-2813-9812-1823 → 2938 1298 1292 2121
Data Masking	Redacting PII in databases ex: **** **** **** 9393

Lesson 4: Identity and Access Management (IAM)

1. Authentication

- **Authentication Design**
  - **CIA Triad Alignment**: Confidentiality (secure credentials), Integrity (no bypass), Availability (no undue delays).
  - **Factors of Authentication**:
    - **Knowledge**: Passwords, PINs.
    - **Ownership**: Hardware tokens (OTP, FIDO U2F), soft tokens (SMS, authenticator apps).
    - **Inherence**: Biometrics (fingerprint, facial recognition).
    - **Location**: Geolocation/IP-based.
- **Password Security**
  - **Concepts**: Length, complexity, aging, reuse history, NIST guidance (no hints, longer phrases).

Concept	Key Difference	When to Use
Length	Total number of characters	Always; longer = stronger
Complexity	Mix of letters, numbers, symbols	Optional if length is strong
Aging	Forces periodic password changes	Only if breach is suspected
Reuse History	Blocks reuse of recent passwords	If aging is enforced

NIST Guidance	Modern best practices (no aging, allow phrases)	Always follow
Hints	Clues to remember passwords	Avoid completely
Passphrases	Long, memorable phrases	Recommended over complex strings

    - **Password Managers**: OS/browser-based, third-party (cloud/plugins), per-site generation.
- **Multifactor Authentication (MFA)**
    - **True MFA**: Combines different factors (password + biometric).
    - **Biometrics**:
        - Enrollment process, FAR/FRR rates, throughput/cost considerations.
    - **Hard Tokens**: Smart cards, OTP fobs, FIDO U2F security keys.
    - **Soft Tokens**: SMS, email, push notifications (interception risks).
- **Passwordless Authentication**
    - Public/private key pairs (no PKI required).
    - Local gestures (biometric/PIN for proof of presence).
    - Attestation for authenticator trust.

---

2. Access Management

- **Access Control Models**
    - **Discretionary (DAC)**: Owner-managed ACLs (vulnerable to privilege abuse).
    - **Mandatory (MAC)**: System-enforced labels/clearances.
    - **Role-Based (RBAC)**: Permissions tied to roles/groups.
    - **Attribute-Based (ABAC)**: Context-aware (user/object attributes).
    - **Rule-Based**: System-defined rules (time/location policies).
- **Least Privilege Principle**
    - Minimal permissions, auditing for creep.
    - **Authorization Challenges**: Insufficient permissions vs. over-provisioning.

Authorization Challenge	Insufficient Permissions	Over-Provisioning
Definition	Users lack necessary access to perform tasks.	Users have excessive permissions beyond their role.
Impact	Reduced productivity; frequent access requests.	Increased attack surface; privilege abuse risks.
Common Causes	Overly restrictive policies; poor role design.	Lack of least privilege enforcement; role creep.
Security Risk	Low (but frustrates users).	High (elevated risk of insider/malicious threats).
Remediation	Regular access reviews; just-in-time provisioning.	Role-based access control (RBAC); periodic audits.

- **Account Lifecycle**
    - **Provisioning**: Identity proofing, credential issuance, asset allocation.
    - Provisioning is the process of setting up a service according to a standard procedure or best practice checklist. Linking multiple systems together can increase the **automation** of onboarding procedures.
    - **Deprovisioning**: Disabling accounts/roles upon exit.
- **Account Restrictions**
    - **Location-Based**: Network/IP, geolocation.
    - **Time-Based**: Logon hours, temporary permissions.
- **Privileged Access Management (PAM)**

- **Zero Standing Privileges**: Ephemeral credentials, just-in-time access.
- **Secure Admin Workstations**: Vaulting/brokering credentials.

---

3. Identity Management

- **Authentication Providers**
  - **Local**: Windows (NTLM/Kerberos), Linux (`/etc/passwd`, `/etc/shadow`, PAM).
  - **Network/Remote**: LDAP, directory services.
- **Directory Services**
  - **LDAP/X.500**: Distinguished names (`CN=User, OU=Dept, DC=org`).
  - **Active Directory**: Group Policy Objects (GPOs).
- **Single Sign-On (SSO)**
  - **Kerberos**:
    - Key Distribution Center (KDC), Ticket-Granting Tickets (TGTs).
    - Mutual authentication for service tickets.

      Key Distribution Center (KDC)

      The **KDC** is like a security guard for a network. It checks your ID (authentication) and gives you a temporary pass (TGT) to request access to other areas.

      Ticket-Granting Ticket (TGT)

      The **TGT** is that temporary pass. You show it to the KDC to get another ticket (service ticket) for specific resources (like email or files).

      How It Works

      1. **Login**: You prove who you are to the KDC.
      2. **Get TGT**: KDC gives you a TGT (time-limited pass).
      3. **Request Access**: Show TGT to get a **service ticket** for apps/files.
      4. **Use Service**: Show the service ticket to access what you need.

      Why It's Secure:

      - Tickets expire quickly.
      - No passwords are sent over the network after login.

- **Federation**
  - **Identity Providers (IdP) & Service Providers (SP)**: SAML, OAuth.
  - The Open Authorization (OAuth) protocol is a system that facilitates the sharing of information (resources) within a user profile between sites. OAuth can be used to implement SSO by allowing users to log in once and access multiple applications without passing credentials through to each piece of software. OAuth can be integrated with other mechanisms to provide SSO capabilities and also supports OpenID Connect (OIDC) tokens to enhance identity verification when needed.

- **SAML**: XML-based assertions (signed, HTTPS/SOAP).
- Security assertion markup language (SAML) allows for federating a network or cloud system. SAML assertions and claims between the principal, the relying party, and the identity provider use eXtensible Markup Language as their structure.
- **OAuth**: RESTful APIs, JWT tokens for authorization (not authentication).

Lesson 5: Enterprise Network Architecture

1. Network Infrastructure & Security Zones

Key Concepts:

- **OSI Model Layers**:
  - **Layer 1 (Physical)**: Cabling, MAC addresses.
  - **Layer 2 (Data Link)**: VLANs, switches (MAC filtering, 802.1X).
  - **Layer 3 (Network)**: IP routing, subnets, firewalls.
  - **Layer 4/7 (Transport/Application)**: TCP/UDP, HTTP/DNS.

OSI layers (1–7) in the context of unauthorized access and network segmentation weaknesses

Layer 1 – Physical

> Allows unauthorized hosts to connect to physical wall ports or wireless networks and communicate with hosts within the same broadcast domain.

Layer 2 – Data Link

> Allows unauthorized hosts to interact at the MAC address level, possibly enabling MAC spoofing, VLAN hopping, or man-in-the-middle attacks within a local segment.

Layer 3 – Network

> Allows unauthorized hosts to obtain a valid IP address, possibly by spoofing, and communicate with hosts in other network zones or subnets.

Layer 4 – Transport

> Allows unauthorized hosts to establish connections to TCP or UDP ports, potentially accessing services at the transport level regardless of IP-level restrictions.

Layer 5 – Session

> Allows unauthorized hosts to establish or hijack sessions, possibly resuming or injecting data into existing communications, impacting session management and persistence.

Layer 6 – Presentation

> Allows unauthorized hosts to bypass or exploit encoding/encryption mechanisms, such as attempting to decrypt SSL/TLS traffic or manipulate data format layers (JSON/XML attacks).

Layer 7 – Application

> Allows unauthorized hosts to interact directly with application services, potentially exploiting vulnerabilities in protocols or applications like HTTP, FTP, DNS, etc.

- **Security Zones**:
  - **Public/Private Zones**: Segment traffic (guest vs. internal networks).
  - **VLANs**: Logical isolation (VLAN 10 for HR, VLAN 20 for Finance).

  VLANs with ACLs create secure segments, providing effective internal traffic control without affecting other layers. This approach not only enhances network performance but also significantly improves security by isolating different network segments

Security Controls:

- **Port Security**: Disable unused ports, MAC filtering, 802.1X (EAP/RADIUS).
- **Physical Isolation**: Air-gapped networks (no external connectivity).

  Physical Isolation means keeping critical systems (like nuclear plants or military networks) completely disconnected from external networks (air-gapped) to block cyberattacks. However, risks remain, especially from **infected USB drives** (like the Stuxnet worm) or insiders smuggling data out. To secure these systems, disable unused USB/network ports, use encryption for removable media, and monitor device access. While air-gapping blocks remote hackers, it's not foolproof—strong physical controls (like Faraday cages) and strict policies are needed to prevent data leaks or sabotage. **Key takeaway**: Isolation reduces risk but requires extra safeguards against physical threats like malicious USB devices.

  > Establishing separate, secure areas for network equipment is a fundamental aspect of physical isolation. It helps limit access to critical infrastructure, thereby enhancing its security.

2. Network Security Appliances

Firewalls:

- **Packet Filtering (Layer 3)**: Blocks by IP/port.
- **Stateful Inspection (Layer 4)**: Tracks TCP handshakes.
- **NGFW (Layer 7)**: Deep packet inspection (blocks malware/exploits).
- **Unified Threat Management (UTM)**: Combines firewall, IPS, anti-malware.
- Organizations actively create a balance between enhanced security and manageable complexity when they deploy Unified Threat Management **UTM** devices internally while also maintaining Next Generation Firewalls **NGFW** at network boundaries.

Other Appliances:

- **IDS/IPS**:
  - **IDS (Passive)**: Alerts on threats.
  - **IPS (Active)**: Blocks threats inline.
- **Proxy Servers**:
  - **Forward Proxy**: Filters outbound traffic (block social media).
  - **Reverse Proxy**: Protects inbound traffic (load balancing).
- **Load Balancers**: Distributes traffic across servers (round-robin, health checks).
- **Web Application Firewall (WAF)**: Blocks SQLi/XSS attacks.

Factor	NGFW	WAF
Purpose	Protects the **entire network** (all traffic).	Protects **web apps only** (HTTP/HTTPS).
Best For	Blocking malware, exploits, and unauthorized access across **all protocols**.	Stopping **web-specific attacks** (SQLi, XSS, API abuse).
Layer 7 Focus	Inspects **all app-layer traffic** (FTP, DNS, HTTP).	Focuses **only on HTTP/HTTPS** (web forms, APIs).
Deployment	Network perimeter (inline).	In front of web servers (reverse proxy).
Example Use Case	Blocking ransomware over SMB or phishing emails.	Preventing credit card theft via a hacked login page.

The **network perimeter** is the boundary between a private internal network (a company's systems) and untrusted external networks (the internet). It's the "front line" of defense where security controls like **firewalls**, **IDS/IPS**, and **gateways** are placed to:

1. **Block unauthorized access** (hackers).
2. **Filter malicious traffic** (malware, DDoS attacks).
3. **Monitor inbound/outbound traffic**.

Key Components of a Network Perimeter

Component	Purpose	Example Tools
Firewall	Blocks unwanted traffic (IPs/ports).	Palo Alto, Cisco ASA

NGFW	Adds Layer 7 inspection (apps/users).	FortiGate, Check Point
IDS/IPS	Detects/stops attacks.	Snort (IDS), Suricata (IPS)
Proxy Server	Filters web traffic (URLs/content).	Zscaler, Squid
VPN Gateway	Secures remote access.	OpenVPN, WireGuard

Placement & Attributes:

- **Inline vs. TAP**: Inline devices (firewall) block traffic; TAPs monitor.
- **Fail-Open vs. Fail-Closed**: Prioritize availability or security during failures.

Fail-Open (Fail-Safe)

When a system fails, it **defaults to "open"** (allowing access).

- **Sacrifices security** to keep availability.
- Example: A firewall fails and lets all traffic through to avoid downtime.
- **Risk**: Hackers may exploit the open access, but operations continue.

Fail-Closed (Fail-Secure)

When a system fails, it **defaults to "closed"** (blocking access).

- **Sacrifices availability** to keep security.
- Example: A bank vault locks during a power failure.
- **Risk**: Legitimate users are blocked, but attackers can't get in.

Trade-off:

- **Fail-Open**: "Better to stay online than be secure" (hospitals).
- **Fail-Closed**: "Better to lock down than stay online" (military systems).

Mnemonic:

🚪 **Open** = Sacrifice security for uptime.

🔒 **Closed** = Sacrifice uptime for security.

---

3. VPNs & Remote Access

VPN Types:

- **Remote Access VPN**: Client-to-site (employees working remotely).
- **Site-to-Site VPN**: Branch office to HQ (IPsec tunnel).

  Remote Access VPN connects individual users (like remote workers) to a private network through a client, **Site-to-Site VPN** links entire networks (like branch offices to headquarters) via encrypted tunnels between routers—one secures single devices, the other connects whole locations.

  Short answer:

  - **Remote Access** = 1 user → office.
  - **Site-to-Site** = office ↔ office.

VPN Protocols:

- **IPsec**:
  - **AH (Authentication Header)**: Integrity only.
  - **ESP (Encapsulating Security Payload)**: Encryption + integrity.
  - **Modes**: Transport (host-to-host) vs. Tunnel (gateway-to-gateway).

    Transport Mode (host-to-host) encrypts only the data payload, leaving original IP headers exposed—ideal for direct secure connections (remote desktop).

    Tunnel Mode (gateway-to-gateway) encrypts the entire packet and wraps it in a new header, hiding all original IP info—used for site-to-site VPNs. Transport is faster but less private; Tunnel is slower but more secure.

    IPsec Core Components

Component	Purpose	Key Features
AH (Authentication Header)	Provides **data integrity** (not encryption)	- Anti-replay protection- Verifies packet wasn't modified
ESP (Encapsulating Security Payload)	Provides **encryption + integrity**	- Encrypts payload- Optional integrity checks
IKE (Internet Key Exchange)	Negotiates encryption keys securely	- Establishes VPN tunnels- Uses Diffie-Hellman for key exchange
NAT-T (NAT Traversal)	Allows IPsec to work through NAT devices	- Encapsulates ESP in UDP packets- Fixes NAT compatibility issues

- **TLS/SSL VPNs**: Uses HTTPS for secure web-based access.
- **IKE (Internet Key Exchange)**: Negotiates encryption keys (IKEv2 improves mobile support).

Remote Access Tools:

- **RDP (Remote Desktop Protocol)**: GUI access to Windows systems.
- **SSH (Secure Shell)**: Encrypted command-line access (uses public-key auth).
- **Jump Servers**: Secure gateway for admin access (isolates critical systems).

---

4. Authentication & Access Control

- **802.1X**: Port-based NAC (uses RADIUS for authentication).

  NAC (Network Access Control) is used to **control which devices can connect to a network** based on **security policies**.

  NAC platform: is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and

  grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks

- **RADIUS vs. TACACS+**:
  - **RADIUS**: Combines auth + authz (UDP).
  - **TACACS+**: Separates auth/authz (TCP, Cisco proprietary).

---

5. Architecture Considerations

- **Defense-in-Depth**: Layered controls (firewalls + IDS + encryption).
- **Availability**: Redundancy (load balancers), failover plans.
- **Patch Management**: Critical for firewalls/VPNs to fix vulnerabilities.

Key Diagrams/Tables

Firewall Types Comparison

Type	Layer	Function
Packet Filtering	3	Blocks by IP/port.
Stateful	4	Tracks connections (TCP handshake).
NGFW	7	Blocks malware/exploits in HTTP traffic.

VPN Protocols

Protocol	Use Case	Key Feature
IPsec	Site-to-Site	Encrypts entire packet (ESP).
TLS/SSL	Client-to-Site	Uses HTTPS for web-based access.
IKEv2	Mobile VPNs	Faster reconnects.

🔐 Authentication / Remote Access

Protocol	Port(s)	Stands For	Purpose
IPsec	500 (IKE), 4500 (NAT-T)	Internet Protocol Security	Encrypts network traffic (VPNs)
ESP	Protocol 50	Encapsulating Security Payload	Provides encryption + integrity in IPsec
AH	Protocol 51	Authentication Header	Provides integrity only in IPsec
TLS/SSL	443 (HTTPS), 993 (IMAPS)	Transport Layer Security/Secure Sockets Layer	Secures web traffic and email
SSH	22	Secure Shell	Encrypted command-line access
RDP	3389	Remote Desktop Protocol	GUI remote access to Windows
RADIUS	1812(auth) 1813(acct)	Remote Authentication Dial-In User Service	Centralized authentication for network devices
TACACS+	49	Terminal Access Controller Access-Control System Plus	Cisco's enhanced authentication protocol
HTTP	80	Hypertext Transfer Protocol	Unsecured web traffic
HTTPS	443	HTTP Secure	Encrypted web traffic
DNS	53	Domain Name System	Translates domain names to IPs
FTP	20 (File Transfer Protocol data transfer) 21 (File Transfer Protocol control (command)	File Transfer Protocol	Unsecured file transfers
SFTP	22	SSH File Transfer Protocol	Secure file transfers over SSH
Telnet	23	Terminal Network	Insecure remote login (not used anymore)
LDAP	389	Lightweight Directory Access Protocol	Directory services (like AD)
LDAPS	636	LDAP Secure	LDAP over SSL/TLS

💌 Email

Protocol	Port	Stands For	Use
SMTP	25	Simple Mail Transfer Protocol	Send email (non-secure)
SMTP (SSL)	465	--	Send email over SSL
SMTP (TLS)	587	--	Send email over TLS
POP3	110	Post Office Protocol v3	Download emails (from server to client)
POP3S	995	POP3 Secure	POP3 over SSL
IMAP	143	Internet Message Access Protocol	Sync/view emails on multiple devices
IMAPS	993	IMAP Secure	IMAP over SSL

🌍 Web / Internet

Protocol	Port	Stands For	Use
HTTP	80	HyperText Transfer Protocol	Normal website traffic
HTTPS	443	HTTP Secure	Encrypted web traffic (TLS)
DNS	53	Domain Name System	Translates domain names to IPs
FTP	21	File Transfer Protocol	File transfers
FTPS	990	FTP Secure	FTP over SSL
SFTP	22	SSH File Transfer Protocol	FTP over SSH
TFTP	69	Trivial FTP	Very simple FTP (no login, no security)
NTP	123	Network Time Protocol	Sync clocks on devices

📦 File Sharing / Network Services

Protocol	Port	Stands For	Use
SMB	445	Server Message Block	File sharing (Windows shares)
NetBIOS	137-139	Network Basic Input Output System	Older name resolution/file sharing
SNMP	161	Simple Network Management Protocol	Network monitoring
SNMP Trap	162	--	Device alerts sent to SNMP managers
Syslog	514	System Logging Protocol	Centralized log collection
DHCP	67/68	Dynamic Host Configuration Protocol	Assign IPs automatically

🔒 Encryption / VPN

Protocol	Port	Stands For	Use
IPSec (IKE)	500	Internet Key Exchange	Secure VPN tunneling
L2TP	1701	Layer 2 Tunneling Protocol	VPN tunnel protocol (with IPSec)
PPTP	1723	Point-to-Point Tunneling Protocol	Legacy VPN (not secure)
OpenVPN	1194	--	Open-source secure VPN protocol

Term	Meaning	Scope
VDE (Virtual Desktop Environment)	A **general term** for any environment where a desktop OS is run in a virtualized context—whether hosted locally or remotely.	Broader, includes all types of virtual desktop setups.
VDI (Virtual Desktop Infrastructure)	A **specific implementation** of VDE where the virtual desktops are hosted on centralized servers (often in data centers or the cloud), and accessed	More specific, refers to centralized hosting and delivery

	remotely by users.	model.

Type	Use Case	Key Advantage	Security+ Tip
VDI	Centralized desktop delivery for users	Centralized control, secure remote work	Ideal for BYOD and remote environments
App Virtualization	Stream specific apps without full desktop	Lightweight, easy deployment	Secure access to sensitive apps only
Containerization	Isolate apps/services (DevOps, microservices)	Fast, portable, efficient	Often used with cloud/microservices
VM	Full OS sandboxing or testing	Strong isolation	Great for malware analysis labs or secure testing
Thin Client	Lightweight endpoint for VDI access	Minimal attack surface	Common in secure terminals or kiosks

Lesson 6: Cloud & Zero Trust

1. Cloud Infrastructure

A. Cloud Deployment Models

Multi-Tenant = "Shared Elevator" (saves money, but crowded).
Single-Tenant = "Private Elevator" (only yours, but costly).

Model	Description	Use Case	Security Considerations	Example Providers
Public	Multi-tenant architecture where compute/storage resources are shared among multiple organizations. Resources are provisioned dynamically with pay-as-you-go pricing.	- Startups needing rapid scaling- Web applications with variable traffic	- Relies on virtualization isolation (hypervisor security)- Customer responsible for data encryption & IAM	AWS, Azure, Google Cloud
Private	Dedicated infrastructure for a single organization, either:- On-premises (self-managed)- Hosted (3rd party manages dedicated hardware)	- HIPAA-compliant healthcare systems- Government classified data	- Full control over physical security- Higher cost for dedicated resources	VMware Private Cloud, OpenStack
Hybrid	Integrates public cloud scalability with private cloud security through:- VPN/leased lines for connectivity- Unified management platforms	- Retail chains (POS on-prem + analytics in cloud)- Financial institutions with legacy mainframes	- Requires secure API gateways- Data gravity challenges	AWS Outposts, Azure Stack
Community	Shared infrastructure for organizations with common compliance/security needs (CJIS for law enforcement)	- Research consortiums- Municipal government systems	- Joint responsibility for security policies- Limited vendor options	IBM Cloud for Government

B. Cloud Service Models

Model	Description	Example	Responsibility (Customer vs. Provider)
IaaS	Infrastructure as a Service (rent VMs, storage)	AWS EC2, Azure VMs	Customer: OS, apps, dataProvider: Hardware, networking
PaaS	Platform as a Service (dev tools, databases)	Heroku, Google App Engine	Customer: Apps, dataProvider: OS, runtime

SaaS	Software as a Service (ready-to-use apps)	Office 365, Salesforce	Customer: just use it bruh DataProvider: Everything else
FaaS	Function as a Service (serverless)	AWS Lambda, Azure Functions	Customer: CodeProvider: Execution environment

C. Cloud Security Considerations

- **Shared Responsibility Model**:
  - **Provider**: Physical security, hypervisor, DDoS protection.
  - **Customer**: Data encryption, IAM, OS patching.

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Comparison Guide	CIS Foundations Benchmarks
Data classification and accountability	Customer	Customer	Customer	Customer	Customer	Customer	Customer
Client and end-point protection	Customer	Customer	Customer	Customer	Customer	Customer	Customer
Identity and access management	Customer	Customer	Customer	Customer	Customer	Customer	Customer
Application-level controls	Customer	Customer	Provider	Provider	Provider	Provider	Provider
Network controls	Customer	Customer	Provider	Provider	Provider	Provider	Provider
Host infrastructure	Customer	Provider	Provider	Provider	Provider	Provider	Provider
Physical security	Provider	Provider	Provider	Provider	Provider	Provider	Provider

Cloud Service Provider = Responsibility matrix

- **Key Technologies**:
  - **SDN (Software-Defined Networking)**: Separates control/data planes for flexible security policies.
  - **SD-WAN**: Securely connects distributed networks over the internet.
  - **SASE (Secure Access Service Edge)**: Combines SD-WAN + Zero Trust (Zscaler).

1. Need to automate a big network? → **SDN**
2. Connecting multiple offices? → **SD-WAN**
3. Have remote workers and cloud apps? → **SASE**

Technology	What It Does	When To Use It
SDN (Software-Defined Networking)	Turns network hardware (like switches) into "dumb" traffic movers, while a central controller makes all decisions.	- When you want to automate and centrally manage a large network (data centers, campuses)- When you

		need dynamic security rules (automatically isolating infected devices)
SD-WAN (Software-Defined Wide Area Network)	Replaces traditional expensive network connections (like MPLS) with smart internet links that automatically choose the best path.	- For businesses with multiple locations (stores, branches) needing reliable, secure connections- When moving from old MPLS networks to cheaper internet-based solutions
SASE (Secure Access Service Edge)	Delivers both networking and security as a single cloud service, combining SD-WAN with Zero Trust protection.	- For companies with remote workers needing secure access to cloud apps- When you want to simplify security (one cloud service instead of multiple hardware devices)

2. Zero Trust Architecture (ZTA)

Core Principles

Principle	What It Means	Real-World Example
"Never Trust, Always Verify"	Every access request is treated as untrusted, even if it comes from inside the network.	An employee accessing HR systems must re-authenticate every time, even from the office network.
Microsegmentation	Divides the network into tiny, isolated zones to contain breaches.	The finance department's servers can't communicate with marketing servers without explicit permission.
Continuous Monitoring	Checks user/device behavior in real-time for anomalies.	If a device suddenly tries to access sensitive data at 3 AM, access is blocked.

Key Components (NIST SP 800-207)

Component	Role	Example Technologies
Policy Engine	The "brain" that decides access based on risk.	- Risk-based authentication tools (Okta, Azure AD Conditional Access)
Policy Administrator	Enforces the Policy Engine's decisions.	- Identity and Access Management (IAM) systems
Policy Enforcement Point (PEP)	The "gatekeeper" that allows/denies access.	- Next-Gen Firewalls (Palo Alto, Fortinet)- Cloud Access Security Brokers (CASB)

Why Zero Trust? (Key Drivers)

Driver	Impact
Cloud Adoption	Traditional perimeter security fails when data lives in AWS/Azure.
Remote Work	Employees access systems from everywhere (home, cafes, airports).
IoT Proliferation	Smart devices (cameras, sensors) are easy targets for hackers.

How Zero Trust Works in Practice

Step-by-Step Example:

1. A remote employee tries to access payroll files.
2. The **Policy Engine** checks:
   - Who they are (MFA verification)
   - Their device security (patched? encrypted?)
   - Location/time of access (normal work hours?)
3. The **Policy Administrator** grants limited access ("view only").
4. The **PEP** (a firewall) enforces this by filtering traffic.
5. **Continuous monitoring** detects if they suddenly download 1TB of data → blocks the session.

Zero Trust vs. Traditional Security

Feature	Traditional Security	Zero Trust
Trust Model	"Trust but verify" (safe inside the network)	"Never trust" (verify everything)
Network Focus	Defends the perimeter (castle walls)	Protects each resource (every room has a lock)
Best For	On-premises networks	Cloud, remote work, hybrid environments

Option	When to choose	Meaning
Secured zones	Choose when the question is about **network/data segmentation**	Isolates parts of the network to control data access
Threat scope reduction	Choose when the question asks about **risk minimization or attack surface**	Reduces how much harm an attacker can do

Implementation Checklist

1. **Identify sensitive data** (what needs most protection?).
2. **Map access flows** (who needs what?).
3. **Deploy microsegmentation** (isolate critical systems).
4. **Enable MFA everywhere** (no more password-only access).
5. **Monitor continuously** (SIEM tools like Splunk).

3. Embedded Systems & IoT

Key Risks

- Limited compute power → Weak encryption.
- Default credentials → Easy exploitation.
- Unpatchable firmware → Long-term vulnerabilities.

Security Frameworks

- **IoTSF (Internet of Things Security Foundation)**: Best practices for IoT devices.
- **ETSI IoT Standards**: EU guidelines for consumer IoT security.

Industrial Systems (ICS/SCADA)

- **Components**: PLCs, HMIs, data historians.
- **Threats**: Stuxnet-style attacks targeting critical infrastructure.

The industrial sector can refer specifically to mining and refining raw materials involving hazardous high heat and pressure furnaces, presses, centrifuges, and pumps.

4. Resilient Cloud Architecture

Concept	Description	Example
Geo-Redundancy	Data replicated across regions (AWS S3 Cross-Region Replication)	Disaster recovery
Auto-Scaling	Dynamically adjusts resources based on demand (Kubernetes pods)	Handling traffic spikes
Containerization	Isolates apps in lightweight environments (vs. VMs)	Docker, Kubernetes

Aspect	Centralized Architecture	Decentralized Architecture

Structure	All computing/resources managed in one central system	Resources/services distributed across multiple systems
Control	Centralized control and decision-making	Independent or loosely coordinated control
Security	Easier to enforce policies and monitor threats	Harder to manage, increased attack surface
Attack Surface	Smaller (fewer entry points)	Larger (more nodes = more targets)
Data Storage	Centralized (in a data center or main server)	Distributed across multiple locations
Scalability	Can bottleneck under heavy load	Easier to scale horizontally
Fault Tolerance	Single point of failure (unless redundancy is built in)	More resilient—failure of one node doesn't stop the system
Performance	High in controlled environments	Varies, may suffer from synchronization or latency issues
Implementation Cost	Generally lower to start, simpler infrastructure	Higher initial complexity and cost
Example Use Cases	Banking systems, corporate intranets, internal ERP	Blockchain, P2P networks, distributed cloud systems
Best Use For	Environments needing **tight control and security**	Environments needing **resilience and global access**

Architecture Models – Core Comparison

Model	Purpose	Key Characteristics
Client-Server	Centralized control and service delivery	Centralized, easy to manage, scalable, single point of failure
Peer-to-Peer (P2P)	Decentralized resource sharing among nodes	No central server, scalable, hard to secure and manage
Hybrid	Combine control and flexibility of client-server & P2P	Balanced model, moderate security, more complex to implement
Monolithic	All-in-one application or system	Tightly coupled, simple deployment, poor modularity, difficult to scale and maintain

Lesson 7: Resiliency and Site Security

1. Asset Management

A. Asset Tracking

Concept	Stands For	Purpose
CMDB	Configuration Management Database	Tracks IT assets and relationships (servers, software licenses).
MDM	Mobile Device Management	Manages/secures smartphones/tablets (remote wipe, policy enforcement).
Cloud Discovery	Automated cloud asset detection	Identifies shadow IT (unauthorized SaaS/IaaS usage).

B. Data Protection & Backups

Backup Type	Description	RPO/RTO	Use Case
Full Backup	Complete copy of all data	Slow RTO, High Storage	Baseline recovery
Incremental	Backs up changes since last backup	Fast RTO, Less Storage	Frequent backups
Differential	Backs up changes since last full backup	Moderate RTO	Mid-tier recovery

Attribute	Incremental	Differential	Image	Storage Area Network (SAN)
What It Backs Up	Only data changed since the **last backup**	All data changed since the **last full backup**	A full snapshot of the **entire system** (OS, files, apps, etc.)	Not a backup type; provides **centralized storage infrastructure**

Backup Speed	Fast	Moderate	Slow	N/A (depends on the backup solution used with SAN)
Recovery Speed	Slow (requires full + all incrementals)	Moderate to fast (requires full + latest differential)	Fast (restores entire system image)	N/A
Storage Usage	Most efficient (smallest size)	Moderate (grows with time since last full backup)	High (due to full system copy)	Varies based on implementation
When to Use	When quick, frequent backups and minimal storage are needed	When balancing backup time with faster restore capabilities	For full system recovery or disaster recovery scenarios	In enterprise environments needing high-performance centralized backup storage
Key Difference	Fast backup, slow restore	Faster restore than incremental, but backups grow over time	Captures everything for full system restore (bare-metal recovery)	Storage system used to support and optimize backup operations

C. Advanced Data Protection

Method	How It Works	Example
Snapshots	Point-in-time system state	Hyper-V, VMware
Replication	Real-time data sync to another site	SAN replication

Replication is the process of **copying data from one location to another**, typically in **real-time** or on a **schedule**, to ensure **data availability and redundancy**.

Journaling is the practice of **recording changes or transactions before applying them**, usually in **filesystems** or **databases**, to help with **recovery** and **integrity**.

Database mirroring is a **high-availability** feature used to **increase data reliability** and **minimize downtime**.

D. Secure Data Destruction

Method	Standard	When Used
DoD 5220.22-M	3-pass overwrite	High-security erasure
Degaussing	Magnetic wipe	HDDs/tapes
Shredding	Physical destruction	SSDs, old hardware

2. Redundancy Strategies

Concept	What It Is	Keyword to Remember	What to Look For on Exam
Continuity of Operations (COOP)	Plan to keep critical business functions running during/after a disaster	*Keep business running*	Scenario talks about disasters, keeping systems available
Backups	Copy of data to restore in case of loss or disaster	*Data loss recovery*	Mention of restoring systems/data after failure
COOP Testing	Regular testing to ensure the plan works when needed	*Validate plan works*	Keywords like **exercise, drill, test**
COOP Updating	Adjusting the plan as systems or threats change	*Keep plan current*	Look for **reviewing or updating** the continuity plan
Capacity Planning	Estimating future needs to prevent bottlenecks during normal or crisis ops	*Future resources ready*	Look for **resource planning, scaling, forecasting**

Aspect	COOP (Continuity of Operations Planning)	BCP (Business Continuity Planning)
Main Focus	Keep essential operations running	Keep the entire business running
Scope	Specific to critical functions (emergency services)	Covers all business areas (IT, staff, services)
Goal	Ensure core operations continue without disruption	Ensure the business as a whole can recover quickly
Used By	Government, public services, emergency organizations	Private companies, all industries
Example	Police and emergency services during a disaster	A company's plan to recover data and customer service after a cyberattack

Risk / Concept	What It Means	Keyword to Remember	When to Choose on Exam
People Risks	Loss of key staff, over-reliance on individuals	*Staff loss or gaps*	Scenario involves critical staff quitting, burnout, or unavailable roles
Cross-Training	Training others to cover key roles in absence	*Skill redundancy*	If asked about **resilience or coverage when someone leaves**
Remote Work Plans	Ability for staff to work from home if needed	*Offsite work continuity*	Choose when scenario involves **disruption to physical offices**
Alternative Reporting Structures	Backup management chains to maintain leadership if someone is unavailable	*Backup leadership*	Scenario where **management is disrupted**
Changes in Workforce Capacity	Increase or decrease in staffing levels	*Staff level change*	Look for references to **team size, workload, or organizational shifts**
Rapid Hiring	Bringing in staff quickly to meet urgent demands	*Fast expansion*	Use when scenario mentions **scaling quickly, growth, or shortages**
Layoffs	Reducing staff due to budget or restructuring	*Downsizing risks*	Scenario involves **staff cuts, reduced support, or role gaps**

A. High Availability (HA) & Fault Tolerance

Type	How It Works	Example
Active/Active	All nodes handle traffic	Load-balanced web servers
Active/Passive	Backup nodes take over if primary fails	Database clusters

Clustering refers to the use of **multiple servers (nodes)** that work together to provide **high availability**, **load balancing**, and **fault tolerance** for services or applications. If one node fails, another can take over, minimizing downtime.

Active/Passive (A/P) Clustering

- One node is **active**, handling all requests.
- One or more nodes are **passive** (standby) and take over only if the active node fails.
- Minimizes resource usage but has **slightly slower failover**.
- **Use case:** Database servers or licensing systems where consistency is more important than performance.

Active/Active (A/A) Clustering

- **All nodes are active** and share the processing load.
- If one fails, the rest **absorb the load**.

- Improves performance and availability, but can be **more complex** to manage.
- **Use case:** Web servers, application servers, load-balanced environments.

Application Clustering

- A specific form of clustering where **applications** (not just servers) are clustered.
- The application state and data are shared between nodes.
- Requires **application-level support** (e.g., clustered database or clustered file system).
- **Use case:** Critical applications like CRM, ERP, or clustered SQL databases.

Feature	Active/Passive (A/P)	Active/Active (A/A)	Application Clustering
Node Usage	One active, others on standby	All nodes active	Depends on application design
Performance	Lower (only one node handles load)	Higher (load is distributed)	Depends on application-level distribution
Failover Speed	Moderate (requires role switching)	Fast (remaining nodes already active)	Can be fast if designed correctly
Complexity	Simple to manage	More complex	Depends on the app; usually more complex
Resource Utilization	Less efficient (standby resources idle)	Efficient (all nodes contribute)	Varies
Typical Use Cases	Database, licensing servers	Web servers, load-balanced apps	Cluster-aware apps (e.g., clustered SQL Server)
Requires Virtual IP	Yes	Yes	Usually yes, or application-specific mechanism

B. Site-Level Resiliency (Disaster Recovery Sites)

Type	Cost	Setup Time	Description	Good For...
Real-time Recovery	$$$$ Extremely High	Instant (0ms)	Continuous synchronous replication with zero data loss	Mission-critical systems (stock trading, 911 dispatch)
Hot site	$$$ High	Immediate (Minutes)	Fully equipped, up-to-date, ready to take over instantly.	When downtime must be minimal
Cloud	$$$ Moderate	Fast (Minutes)	Everything is always live and mirrored. Instant recovery.	When downtime is not acceptable (0 RTO/RPO)
Warm site	$$ Moderate	Few hours to 1 day	Partially equipped with some data and systems.	Balanced option for moderate RTO/RPO
Cold site	$ Low	Long (Days)	Just an empty facility with power & internet. Needs setup time.	When cost is key and delay is acceptable

C. Power Redundancy

Component	Purpose
UPS (Uninterruptible Power Supply)	Provides short-term battery backup to keep systems running during brief power interruptions and allows safe shutdown or switch to generator power during extended outages.
Generator	Supplies long-term electrical power during prolonged outages by converting fuel (diesel, gas, etc.) into electricity, ensuring continuous operation of critical systems.

Dual PSUs (Dual Power Supply Units)	Offers redundancy by using two independent power sources, so if one PSU fails or is disconnected, the other continues to power the server, minimizing the risk of downtime.

Feature	Generator	Uninterruptible Power Supply (UPS)
Purpose	Provides **long-term power** (hours/days) during outages.	Provides **short-term power** (minutes/hours) until generators kick in or systems shut down safely.
Power Duration	Days (with fuel refills).	Minutes to a few hours (battery-based).
Activation Time	10–60 seconds to start.	Instant (no delay).
Use Case	Sustains operations during prolonged outages.	Bridges gaps during power transitions or handles brief outages.
Example	Diesel generators powering a data center for 48+ hours.	UPS keeps servers running for 15 minutes until generators activate.

D. Deception Technologies

Tool	Purpose
Honeypot	A decoy system or server designed to attract attackers, allowing defenders to monitor and analyze malicious behavior without risking real assets.
Honeynet	A network of interconnected honeypots that simulates a full environment, providing deeper insights into attacker tactics, techniques, and procedures (TTPs).
Honeyfile	A decoy file placed on a system (fake spreadsheets, documents) to detect unauthorized access or data exfiltration attempts when opened or moved.
Honeytoken	A fake piece of data (credentials, API keys) planted in systems or databases; if used, it alerts defenders that a breach or data leak has occurred.
Fake Telemetry	Simulated system or network activity data used to mislead attackers, obscure real asset behavior, or to identify and monitor attacker interactions with decoy elements.

E. Testing Resiliency

Test Type	Purpose
Tabletop Exercise	A discussion-based scenario where team members walk through emergency procedures to identify gaps and improve response strategies without disrupting operations.
Failover Test	Simulates a failure of primary systems to ensure backup systems (servers, databases, network paths) can take over seamlessly and maintain service continuity.
Simulation	A controlled, realistic test that mimics actual incidents (cyberattacks, natural disasters) to assess how systems and personnel respond under stress.
Parallel Processing Test	Runs backup systems in parallel with primary systems to verify they can handle live data loads without fully switching over, ensuring readiness without downtime.
Robust Documentation	Ensures that all processes, configurations, and recovery plans are clearly documented and up to date, enabling quick response and consistent recovery during incidents.

3. Physical Security

A. Perimeter Security

Control	Purpose

Fencing	Establishes a physical barrier to restrict unauthorized access and define property boundaries, often used to delay or deter intruders.
Lighting	Enhances visibility in and around secure areas, deters unauthorized access or suspicious behavior, and supports surveillance efforts at night.
Bollards	Sturdy, short vertical posts that block or restrict vehicle access to sensitive areas, preventing vehicle-based attacks or accidental intrusions.

B. Access Control

Method	Stands For
Physical	Tangible barriers like walls, doors, and locks that prevent unauthorized physical access to facilities or equipment.
Electronic	Security systems such as CCTV, motion detectors, and electronic alarms used to monitor and protect facilities.
Access Control Vestibule (Mantrap)	A double-door entry system that allows only one person at a time to prevent piggybacking and tailgating.
Cable Locks	Physical locking mechanisms used to secure laptops and other portable devices to fixed objects, deterring theft.
Access Badges	Identification cards with embedded chips or magnetic stripes used to grant or restrict entry to secure areas based on authorization.
Biometrics	Authentication based on unique physical characteristics such as fingerprints, facial recognition, or retina scans.

C. Monitoring & Alarms

Tool	Purpose
CCTV	Provides continuous video surveillance to monitor activity, deter intrusions, and support incident investigations.
PIR Sensors	Detect motion by sensing changes in infrared radiation, typically used to trigger alarms or activate lighting in secured areas.
Motion Recognition	Uses software algorithms to identify and respond to movement captured by cameras or sensors, enhancing automated security response.
Object Detection	AI-powered visual analysis that identifies specific items (weapons, unattended bags) in a surveillance feed for real-time alerts.
Drones/UAV (Unmanned Aerial Vehicles)	Provide aerial surveillance over large or remote areas, offering live video, thermal imaging, or automated patrols in difficult-to-access zones.

Lesson 8: Vulnerability Management

1. Device and OS Vulnerabilities

- **Legacy Systems**: Older systems no longer supported by vendors; can't receive patches or updates, leaving known vulnerabilities exploitable.
- **End-of-Life (EOL) Systems**: Similar to legacy, these systems are officially retired and pose security risks due to lack of support.

Topic	Legacy Systems	End-of-Life (EOL) Systems
What it means	Old systems still being used, but outdated	Old systems that the company officially stopped supporting
Support from company	Usually no support, but sometimes a little	No support at all
Security updates	Rare or none; may need custom fixes	No updates or fixes available
Security risk	Easy to hack if not protected	High risk because hackers know how to break them
Why still used?	May be too expensive or hard to replace	Usually shouldn't be used anymore
Rules and compliance	Might break security rules	Often breaks security rules
Example	Old factory computer using Windows XP	Windows Server 2008 after Microsoft stopped updates
What to do with it	Try to update or replace it	Replace it as soon as possible
Are they the same?	Similar, but not exactly the same	EOL systems are a type of legacy system

Type / State	Description	Key Concern
EOL (End of Life)	The vendor no longer supports or sells the product.	No security patches or official support.
EOS (End of Support)	The product is no longer maintained — no updates or technical help.	Increased risk of vulnerabilities.
Obsolete	Extremely outdated; typically replaced by multiple generations of tech.	Incompatibility with modern systems.
Unsupported	Not officially supported in the current environment but may still function.	Operational risk if issues occur.
Deprecated	Still works, but its use is discouraged; will likely be removed in future.	Transition planning needed.
Retired	Formally decommissioned and no longer in use within the organization.	Data retention and archival issues.
Legacy	Still in use, but outdated and possibly difficult to maintain or secure.	Needs special handling or migration plan.

- **Firmware Vulnerabilities**: Embedded software flaws in hardware devices that can be difficult to detect or patch.
- **Virtualization Vulnerabilities**: Weaknesses in virtual machines or hypervisors (escape attacks).
- **Application Vulnerabilities**: Security flaws in software installed on devices or OS.
- **Zero-Day Vulnerabilities**: Unknown by vendors and unpatched; attackers exploit before a fix is available.
- **Misconfigurations**:
  - Default credentials left unchanged.
  - Unnecessary open ports/services.

- Poor cloud or system settings.

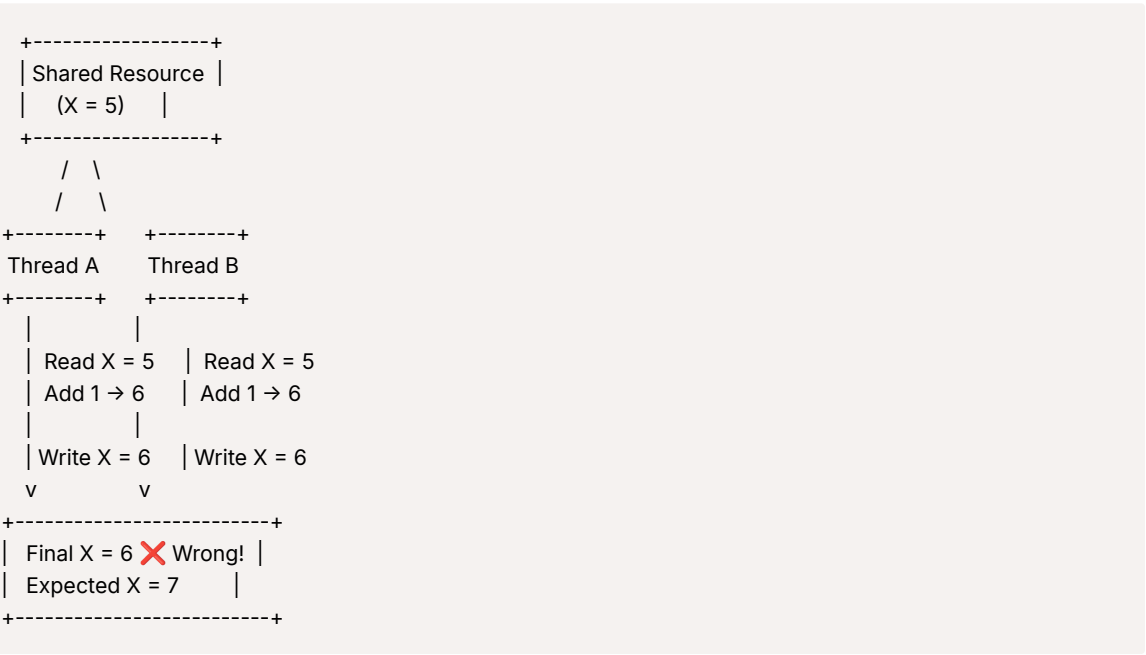
- **Cryptographic Vulnerabilities**:
  - **Weak Keys**: Short or poorly generated keys can be brute-forced.
  - **Deprecated Algorithms**: MD5 and SHA-1 are no longer secure.
  - **Misconfigured Cipher Suites**: Weak or improperly used encryption protocols.
  - **Unprotected Keys**: Keys exposed or stored insecurely.

- **Sideloading**: Installing apps from non-official sources (APK files on Android).
- **Rooting (Android)**: Gaining root privileges; exposes system to risks.
- **Jailbreaking (iOS)**: Removing iOS restrictions to allow custom apps; increases attack surface.

---

2. Application and Cloud Vulnerabilities

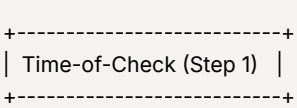
- **Application Vulnerabilities**:
  - **Race Condition**: Flaw where Two processes access the same resource at once and attempt to perform actions in an unexpected order.

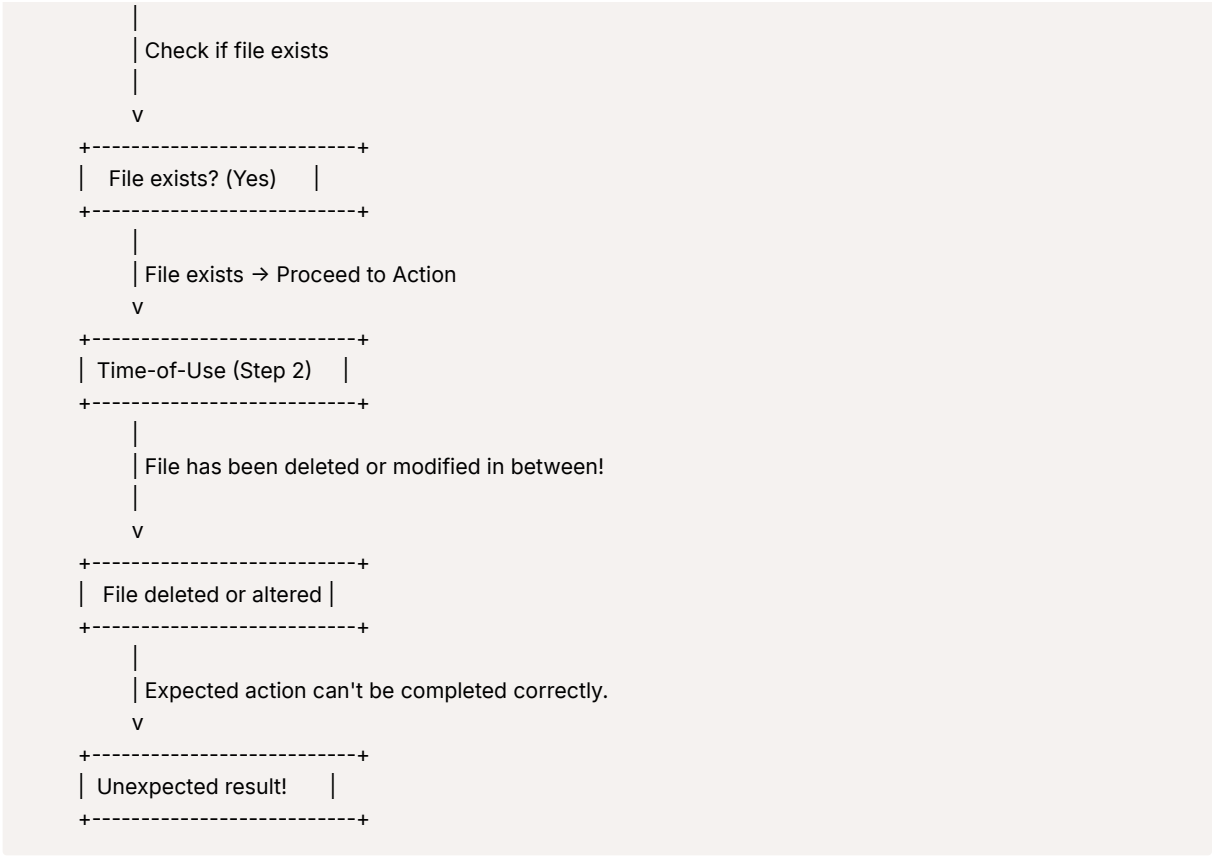


⚠️ Problem: Both threads read X before either writes it.
So they overwrite each other — one increment is lost.

🛠️ Fix: Use a lock/mutex so only one thread writes at a time.

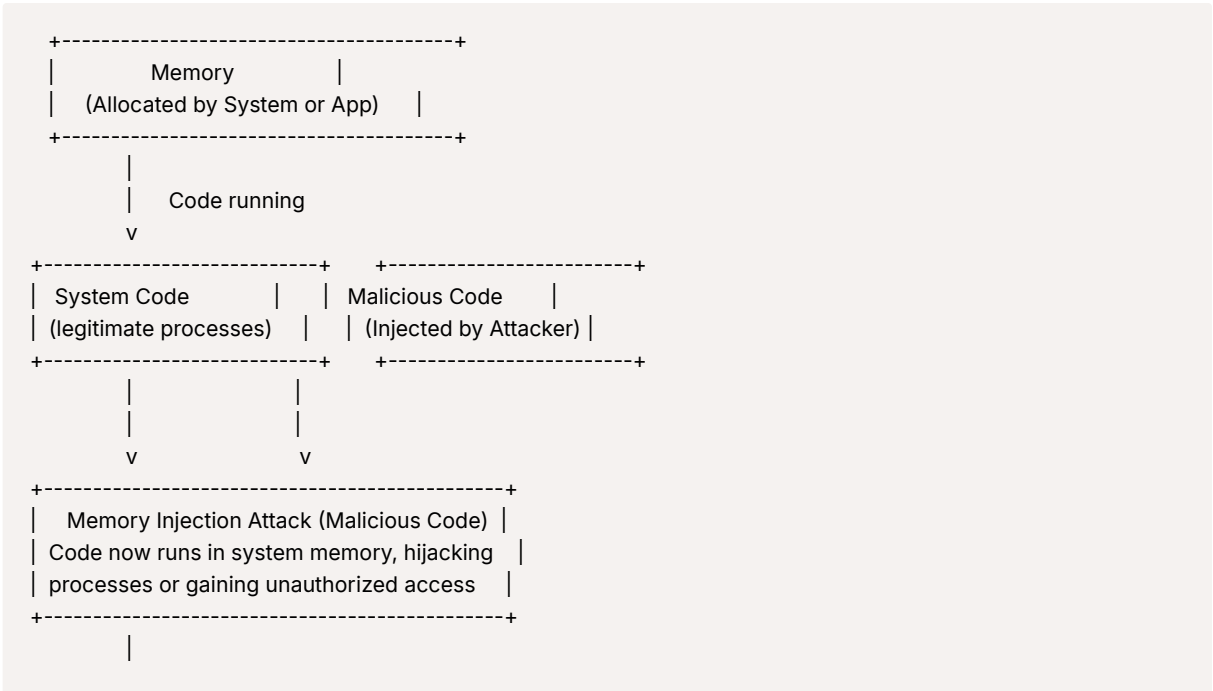
  - **TOCTOU (Time-of-check to time-of-use)**: System state changes between verification and action.





⚠️ **Race Condition**: The system checked the file and assumed it would still be there during the next step. In the time between, the file was changed or deleted.

- **Memory Injection**: Malicious code is injected into memory.



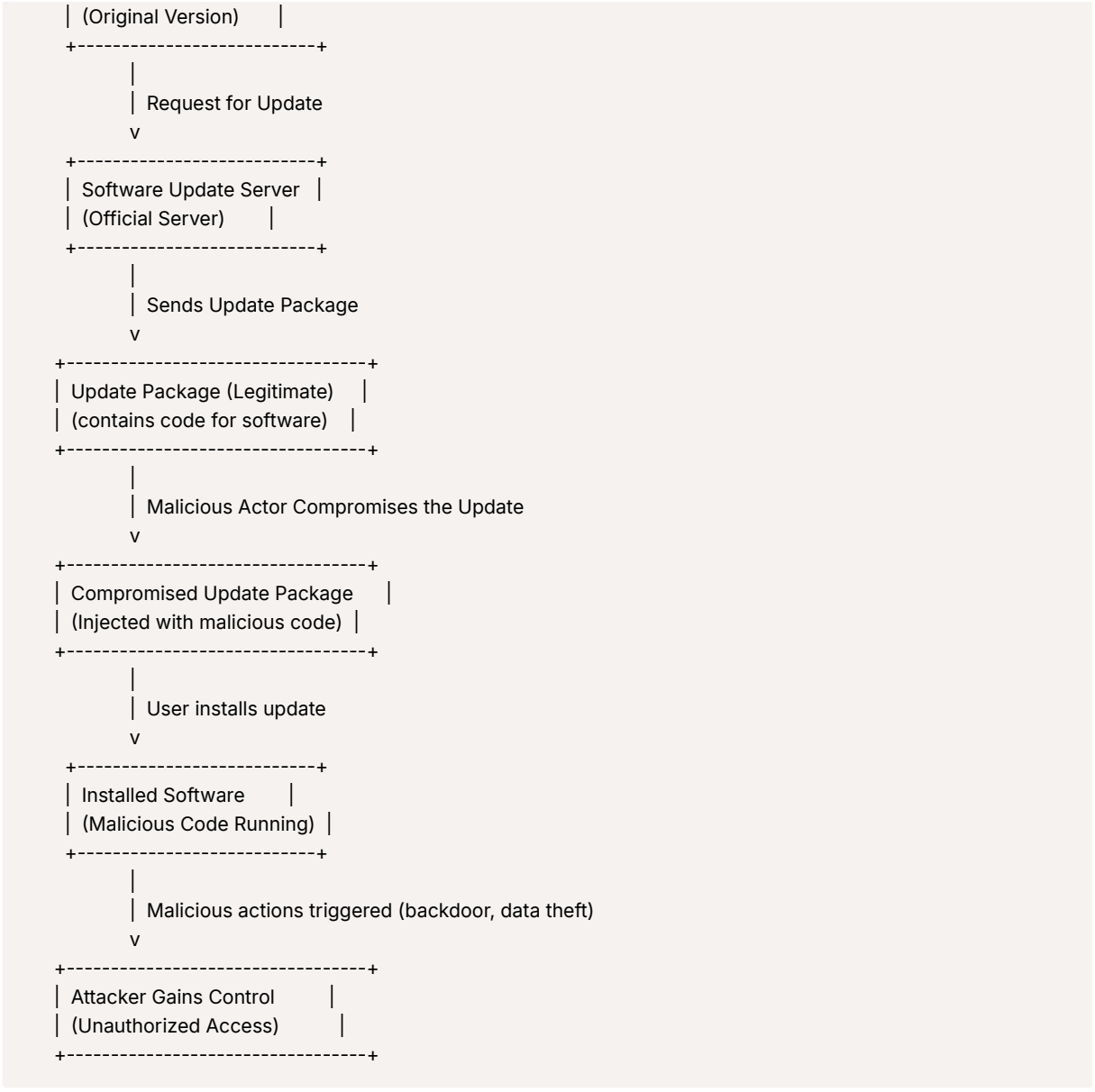
```
        v
  +------------------------+
  |  Unintended Behavior   |
  | privilege escalation   |
  +------------------------+
          |
          v
+------------------------------+
|     Attacker Control         |
|  (Full control over system)  |
+------------------------------+
```

- **Buffer Overflow**: Excess data overflows into adjacent memory.

```
   +--------------------------------------+
   | Buffer (Memory Space for Data)       |
   | (Designed to hold fixed-size data)   |
   +--------------------------------------+
          |
          | Data input (fixed size)
          v
   +-------------------------+
   | Stored Data in Buffer   |
   +-------------------------+
          |
          | Exceeds buffer size
          v
  +-----------------------------+
  | Overflow: Data writes beyond |
  | allocated space and corrupts |
  | adjacent memory              |
  +-----------------------------+
          |
          | Malicious code can be injected here
          v
   +-----------------------------------------+
   | Adjacent Memory(Corrupted or Overwritten)|
   +-----------------------------------------+
          |
          | Leads to unpredictable behavior,
          | potential system crash, or execution
          | of injected code (Exploiting the overflow)
          v
   +-----------------------------------------+
   | Attacker's Malicious Code Executed      |
   +-----------------------------------------+
```

- **Malicious Updates**: Compromised update packages.

```
   +--------------------------+
   | Legitimate Software      |
```



- **Type-Safe Programming Languages**: These languages enforce type rules strictly (like Java, C#, Rust, C++), help prevent memory-related vulnerabilities.

- **Evaluation Scope** (for secure software development):
  - **Security Testing**, **Documentation Review**, **Source Code Analysis**,
  - **Configuration Assessment**, **Cryptographic Analysis**, **Compliance Verification**, **Security Architecture Review**.
- **Web Attacks**: **who need to read this**
  - **XSS (Cross-Site Scripting)**: Injects malicious scripts into web pages.
  - **SQLi (SQL Injection)**: Attacker manipulates SQL queries.
  - **CSRF (Cross-Site Request Forgery)**: Forces users to execute unwanted actions.

- **Cloud-Based Vulnerabilities**:
  - **Cloud Attack Platforms**: Attackers abuse cloud services (launching bots).
  - **Cloud Misconfiguration**: Public S3 buckets, overly permissive access.
  - **Cloud Access Security Brokers (CASBs)**: Help monitor and enforce policies.

Key Term	keys
Cloud Attack Platforms	"Attackers use cloud to launch bots, malware, or DDoS"
Cloud Misconfiguration	"Public S3 buckets", "overly open access", "unauthorized exposure"
CASB (Cloud Access Security Broker)	"Enforce security policies", "monitor cloud app use", "visibility/control"

- **Supply Chain Risks**:
  - Vulnerabilities from vendors (hardware/software).
  - Example: SolarWinds.
  - Tools: SBOM (Software Bill of Materials), Dependency Analysis, Code Signing, Vendor Risk Assessment.

Tool	Purpose	Keyword to Remember	Primary Focus	Extended Description
SBOM (Software Bill of Materials)	Lists all components used in a software product	*What's inside the software*	**Inventory + Visibility**	A formal record of all the open-source and proprietary libraries, packages, and modules used in a piece of software. Helps organizations know exactly what software they're using and identify risky or outdated components.
Dependency Analysis	Scans third-party dependencies for known vulnerabilities	*Are components vulnerable?*	**Vulnerability Detection**	Evaluates the external libraries and packages your software depends on. It checks them against vulnerability databases (like CVE) to detect issues. Often used in CI/CD pipelines to catch issues early.
Code Signing	Confirms that code is authentic and unaltered	*Tampering or legit?*	**Trust + Integrity**	Uses cryptographic signatures to verify that software (binaries, scripts, installers) comes from a trusted source and hasn't been modified. Prevents installation of malicious or tampered code.
Vendor Risk Assessment	Reviews the security practices of third-party vendors	*Is the vendor secure?*	**Vendor Security Practices**	Involves reviewing a vendor's policies, history, certifications, breach record, and controls to ensure they meet security standards. Helps prevent introducing risk via poorly secured suppliers.

---

3. Vulnerability Identification Methods

- **Vulnerability Scanning**:
  - **Nessus**, **OpenVAS** (Greenbone).
  - **Credentialed Scan**: Uses login credentials for deeper checks.
  - **Non-Credentialed Scan**: Surface-level scan, less accurate.
  - **Web/App Scanners**, **Package Monitoring**.
- **Threat Feeds**:
  - Real-time updates on emerging threats.
  - Examples: MITRE ATT&CK, IBM X-Force, Mandiant, Proofpoint, Abuse.ch.

- Sources: OSINT, ISACs, blogs, forums, dark web.

- **Deep and Dark Web**:
  - **Deep Web**: Not indexed by search engines.
  - **Dark Web**: Anonymous overlay networks (TOR) hosting illicit content.
- **Other Assessment Methods**:
  - **Penetration Testing**:
    - **Unknown** environment: No internal knowledge.
    - Known environment: Full internal knowledge.
    - Partially Known environment: Partial knowledge.
  - **Bug Bounties**: Public vulnerability discovery programs.
  - **Auditing**: Systematic review of configurations and activities.

---

4. Vulnerability Analysis and Remediation

- **Common Vulnerabilities and Exposures (CVE)**:
  - Identifiers for known vulnerabilities.
  - **National Vulnerability Database (NVD)**, **SCAP** used for standardization.

Term/Tool	Purpose	Keyword to Remember	When to Choose It
CVE (Common Vulnerabilities and Exposures)	Standard identifiers for known vulnerabilities	*Known flaws catalog*	Question talks about tracking or identifying known issues
NVD (National Vulnerability Database)	U.S. gov database that uses CVEs, part of SCAP	*Standardized CVE database*	Question mentions government source or CVE scoring
SCAP (Security Content Automation Protocol)	Automates vulnerability management and policy compliance	*Automation + CVE integration*	Look for automation, policy checking

- **CVSS (Common Vulnerability Scoring System)**:
  - 0.1–3.9: Low
  - 4.0–6.9: Medium
  - 7.0–8.9: High
  - 9.0–10.0: Critical

CVSS Score Range	Severity Level	Keyword	When to Choose
0.1 – 3.9	Low	*Low impact*	Minor issues, low urgency
4.0 – 6.9	Medium	*Moderate threat*	Fix needed, but not critical
7.0 – 8.9	High	*Major issue*	Requires fast attention
9.0 – 10.0	Critical	*Severe, urgent*	Patch immediately, very high risk

- **Vulnerability Analysis Factors**:
  - **Prioritization**, **Classification**, **Exposure**, **Environmental Variables**, **Risk Tolerance**.

Factor	What It Does	Keyword to Remember
Prioritization	Focus on most critical vulnerabilities	*What to fix first*
Classification	Group by type, severity, exploitability	*Type/severity grouping*
Exposure	Whether the vulnerability is reachable or public	*Can it be reached?*

Environmental Variables	Organizational context that affects risk	*Unique org factors*
Risk Tolerance	How much risk the organization is willing to accept	*Acceptable risk level*

- **Remediation Practices**:
  - **Patching**
  - **Cybersecurity Insurance**
  - **Network Segmentation**
  - **Compensating Controls**: Alternatives when fixes aren't feasible.
  - **Exceptions/Exemptions**
  - **Validation & Re-Scanning**
  - **Auditing & Reporting**

Method	Description	Keyword to Remember	When to Choose
Patching	Fix the vulnerability with a software update	*Fix available*	Fix is known and available
Cybersecurity Insurance	Transfers financial risk in case of breach	*Risk transfer*	Cost-related risk mitigation
Network Segmentation	Limits access and contains threats	*Limit lateral movement*	Reduce spread, not patching
Compensating Controls	Workaround when patch isn't possible	*Alternative security*	Legacy system, can't patch
Exceptions/Exemptions	Approved non-remediation for low-risk cases	*Documented acceptance*	Risk accepted formally
Validation & Re-Scanning	Verify fix, check if vulnerability still exists	*Did fix work?*	Always after patching
Auditing & Reporting	Track progress, meet compliance	*Documentation + compliance*	Regulatory or policy-based follow-up

---

Lesson 9: Network Security Capabilities

1. Security Baselines

What is Baseline Configuration?
A
baseline configuration is a **standard, secure starting point** for systems, networks, or applications before they are deployed or go into production.

Benchmarks and Secure Configuration Guides

- **Security Baseline**: A collection of standardized, best-practice configurations designed to harden systems (operating systems, network devices, software, cloud instances) against known threats. Baselines cover patching, access controls, logging, monitoring, encryption, password policies, endpoint protection, and more.
- **CIS (Center for Internet Security) Benchmarks**: Community-developed, consensus-based configuration standards for securing various systems and software. Widely used by organizations to implement strong baseline configurations.

- **STIGs (Security Technical Implementation Guides)**: Configuration guides developed by the U.S. Department of Defense to ensure systems are securely deployed and operated within federal networks. Used to enforce strict security postures.
- **Vendor-Provided Guidance**: Security configuration documentation released by hardware/software vendors to help securely deploy their products according to industry standards.
- **SCAP (Security Content Automation Protocol)**: A set of standards maintained by NIST for automating vulnerability management, measurement, and policy compliance evaluation. Enables standardized security reporting and assessment.
- **OpenSCAP**: An open-source framework for compliance monitoring using SCAP standards. Useful for auditing and verifying system configurations.
- **CIS-CAT Pro (CIS Configuration Assessment Tool Pro)**: A tool developed by CIS that scans systems and reports compliance with CIS Benchmarks. Offers detailed remediation guidance.
- **SCC (SCAP Compliance Checker)**: A DoD tool used to assess system compliance with STIGs and SCAP content. Often used in government and defense environments.
- **Configuration Management Tools**:
  - **Puppet, Chef, Ansible**: Automation tools used to deploy, manage, and enforce security baselines across large-scale IT environments. Ensure consistency and compliance with defined configurations.

Standard/Tool	Keywords
Security Baseline	Harden systems, best-practice configurations, patching, access control
CIS Benchmarks	Community-developed, secure configs, industry standard
STIGs	DoD, government, secure deployment, military compliance
Vendor Guidance	Vendor-specific, secure setup, official recommendations
SCAP	NIST, automation, compliance checking, vulnerability management
OpenSCAP	Open-source, SCAP compliance, auditing
CIS-CAT Pro	CIS scanner, compliance reporting, remediation guidance
SCC (SCAP Compliance Checker)	DoD tool, checks STIG/SCAP compliance
Puppet/Chef/Ansible	Automation, configuration management, enforce baselines

---

2. Switch and Router Hardening

- **Change Default Credentials**: Replace factory-default usernames and passwords on all network equipment to prevent unauthorized access using widely known credentials.
- **Disable Unused Ports/Services**: Shut down all physical switch ports and logical services (Telnet, FTP, SNMP) that are not actively in use to reduce the attack surface.
- **Use Secure Management Protocols**:
  - Replace insecure protocols like **Telnet** with **SSH** for encrypted remote management.
  - Use **HTTPS** instead of HTTP for web interfaces.
  - Enable **SNMPv3** over SNMPv1/2 for secure network monitoring.
- **Implement ACLs (Access Control Lists)**:
  - Define traffic rules to **permit or deny** based on IP addresses, ports, and protocols.
  - Use **inbound and outbound ACLs** to limit what traffic enters and leaves interfaces.
- **Enable Logging & Monitoring**:

- Configure syslog servers or SIEM tools to **capture and monitor event logs** for suspicious activity.
- Enable **real-time alerting** for unauthorized access attempts or configuration changes.

- **Configure Port Security**:
  - Restrict the number of MAC addresses allowed on a port.
  - Automatically disable or limit access when an unauthorized device connects.
  - Use features like **sticky MAC addresses**, **shutdown**, or **restrict** modes.
- **Strong Passwords**:
  - Require complex passwords (length, complexity, expiration).
  - Avoid easily guessable credentials.
  - Enforce regular password changes and use of **multi-factor authentication** where available.
- **Physical Security**:
  - Place switches and routers in **locked racks or server rooms**.
  - Restrict physical access to only authorized personnel.
  - Use tamper-evident seals or surveillance for critical infrastructure.

---

3. Server Hardening

- **Disable Unnecessary Services**: Turn off non-essential services and daemons (FTP, Telnet, print services) to minimize the system's attack surface and reduce exploitable entry points.
- **Apply Regular Updates & Patches**: Keep the operating system and installed applications up to date with the latest **security patches** to fix known vulnerabilities and prevent exploitation.
- **Enforce Least Privilege Principle**: Assign users and services **only the minimum level of access** required to perform their tasks. Prevents misuse or compromise of privileged accounts.
- **Use Firewalls & IDS**:
  - **Host-based Firewalls**: Restrict inbound/outbound traffic directly on the server.
  - **Intrusion Detection Systems (IDS)**: Monitor for suspicious activity or policy violations (HIDS like OSSEC).
  - Placing the IDS directly behind the router ensures visibility of all incoming and outgoing traffic, which is crucial for detecting any unusual patterns or potential threats

- **Apply CIS/STIG Baselines**:
- Use **CIS Benchmarks** or **STIGs** to configure the server according to standardized, secure settings.
- Covers areas like file permissions, user policies, services, and logging.
- **Enable Logging & Monitoring**:
  - Enable detailed system and security logs (audit logs, event logs).
  - Forward logs to **SIEM systems** for centralized monitoring and alerting on suspicious behavior.
- **Use Antivirus/Antimalware**:
  - Deploy up-to-date **endpoint protection software** to detect and block malware.
  - Enable **real-time scanning** and scheduled full-system scans.
- **Physically Secure Servers, Racks, and Rooms**:

- Place servers in **locked server racks** or **secure data centers**.
- Implement **access control mechanisms** (keycards, biometrics).
- Monitor with **cameras and alarms** to prevent physical tampering or theft.

---

4. Wireless Security

Installation Considerations

- **Site Surveys & Heat Maps**: Optimize WAP (**Wi-Fi Protected Access)** placement and coverage.

Wireless Encryption Standards:

- **Open**: No encryption; insecure.
- **WEP (Wired Equivalent Privacy)**: Outdated, insecure, 90s very bad
- **WPA/WPA2**: Stronger, still in use.
- Wi-Fi Protected Access (WPA), particularly Wi-Fi Protected Access 3 (WPA3), secures the traffic sent over a wireless network. Based on this scenario, the company needs to encrypt the wireless traffic.
- Wireless access points provide a bridge between a cabled network and wireless hosts, or stations. Access points work at layer 2 of the OSI model. Wireless devices also use MAC addressing at layer 2.

- **WPA3**:
  - Uses **SAE (Simultaneous Authentication of Equals)** for secure key exchange.
  - Includes **Enhanced Open** for public networks.

- **DPP (Device Provisioning Protocol)**: AKA **Easy Connect**; replacement for insecure **WPS (Wi-Fi Protected Setup)**.

Authentication Methods:

- **WPA2/3 Personal**: Pre-Shared Key (PSK).
- **WPA2/3 Enterprise**:
  - Uses **802.1X** authentication.
  - Involves **RADIUS (Remote Authentication Dial-In User Service)** and **EAP (Extensible Authentication Protocol)**.

EAP Type	Full Name	How It Works	Uses Certificates	Security Level	Where/When It's Used
EAP-TLS	EAP - Transport Layer Security	Uses **TLS** and **certificates** on both client + server	Client + Server	Very High	Enterprise Wi-Fi (802.1X), highly secure networks
PEAP	Protected EAP	Server cert + inside tunnel = **MS-CHAPv2** (username/password)	Server only	Medium	Common in enterprise Wi-Fi
EAP-TTLS	EAP - Tunneled TLS	Server cert + tunnel with flexible auth (PAP, CHAP, MS-CHAPv2, etc.)	Server only	Medium–High	Companies needing flexibility with old systems
EAP-FAST	EAP - Flexible Authentication via Secure Tunneling	Uses **PAC (pre-shared key)** instead of certs	(uses PACs instead)	Medium	Cisco networks, fast auth without certificates
LEAP	Lightweight EAP	Uses **MS-CHAPv1**, no tunnel, password sent in weak format	None	Very Low	**Deprecated — never use**

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Setup (WPS)
block other users from using their household Wi-Fi

---

5. Network Access Control (NAC)

- **Purpose**: Validates users/devices before granting network access.
- **Agent-Based NAC**: Requires software on endpoints.
- **Agentless NAC**: Uses network scans and fingerprinting.
- Example tool: **PacketFence** (supports Nessus, OpenVAS, WMI, log parsers).

---

6. Network Controls

Access Control Lists (ACLs):

- Rules defining what traffic is permitted or denied.
- Applied on routers, firewalls, or switches.
- Can control based on:
  - Source/Destination IP
  - Protocols
  - Ports

Screened Subnet (DMZ):

- Isolated network area that separates public services from internal systems.

---

7. Firewalls and UTM

- **NGFW (Next-Generation Firewall)**:
  - Layer 7 (application layer) filtering.
  - Can inspect SSL/TLS, detect malware, block applications.
- **UTM (Unified Threat Management)**:
  - Combines firewall, antivirus, IDS/IPS, content filtering, etc., into one device.

---

8. IDS/IPS

Types:

- **HIDS (Host-Based IDS)**: Monitors single devices.
- **NIDS (Network-Based IDS)**: Monitors traffic across networks.
- **IPS (Intrusion Prevention System)**: Actively blocks threats.

Detection Methods:

- **Signature-Based**: Matches known attack patterns.
- **Anomaly-Based**: Flags behavior outside of established baselines.
- **Behavioral-Based**: Tracks typical user/system behavior.
- **Trend Analysis**
- **NBAD (Network Behavior and Anomaly Detection)**
- **UEBA (User and Entity Behavior Analytics)**

Common Tools:

- **Snort**, **Suricata**, **OSSEC**

9. Web Filtering

- **Purpose**: Restrict web access, block threats.
- **Techniques**:
  - **Agent-Based Filtering**
  - **Centralized Filtering**
  - **URL Scanning & Categorization**
  - **Reputation-Based Filtering**
  - **Block Rules**
  - **HTTPS Decryption/Inspection**
- **Use Cases**:
  - Block malware/phishing sites.
  - Enforce acceptable use policies.
  - Prevent data exfiltration.

Lesson 10: Endpoint Security

1. Endpoint Hardening

Operating System Security

- Apply **CIS Benchmarks** or **STIGs** to harden Windows, Linux, macOS.
- Configure secure **baseline settings**: disable unnecessary services, close open ports, restrict interfaces.
- Use **least privilege**: restrict user and system permissions to only what is necessary.
- Harden **file systems**, enforce **ACLs**, and monitor with **Group Policy** or **SELinux**.

Hardening Techniques

- **Change Defaults**: Remove default credentials and settings.
- **Remove Unnecessary Software**: Reduce attack surface.
- **Protect Physical Ports**: Disable unused USBs, restrict console access.
- **Full Disk Encryption (FDE)**: **BitLocker** — encrypts entire drive.
- **Removable Media Encryption**: Protect data on USBs and external storage.
- **Email Encryption**: Secure sensitive communications.
- **Host-Based Firewalls/IPS**: Prevent unauthorized access.

- **VPNs**: Encrypt traffic from remote devices.

Endpoint Protection

- **Network Segmentation**: Isolate departments or sensitive systems.
- **Isolation**: Quarantine compromised endpoints.
- **Antivirus/Antimalware**: Detect known threats.
- **Patch Management**: Fix vulnerabilities proactively.

Hardening Specialized Devices

- **ICS/SCADA Systems**:
  - Use **network segmentation** and **unidirectional gateways** (data diodes).
  - Enforce **strong authentication**.
- **Embedded Systems & RTOS**:
  - Choose secure hardware/software.
  - Avoid unnecessary network exposure.

---

2. Advanced Endpoint Protection

Technology	Purpose	Key Difference
EDR (Endpoint Detection and Response)	Real-time monitoring and response for endpoint threats.	Focused on individual endpoints.
XDR (Extended Detection and Response)	Centralized view and correlation of threats across endpoints, servers, and networks.	Broader scope than EDR, integrates multiple data sources.
HIDS (Host-Based Intrusion Detection System)	Detects threats on a specific host (logs, files, traffic).	Passive — alerts only.
HIPS (Host-Based Intrusion Prevention System)	Monitors and blocks malicious behavior on the host.	Active — blocks threats in real-time.
UEBA (User & Entity Behavior Analytics)	Detects anomalies in user/system behavior.	Behavior-based; good for insider threat detection.

---

3. Mobile Security

Deployment Models

Model	Definition
BYOD (Bring Your Own Device)	User owns device, used for work. High flexibility, high risk.
COPE (Corporate-Owned, Personally Enabled)	Company-owned device with personal use allowed. Balance of control and user freedom.
COBO (Corporate-Owned, Business Only)	Strict company-only use. High security, low user freedom.
CYOD (Choose Your Own Device)	User selects from pre-approved device list. Mix of control and customization.

Mobile Device Hardening

- **Full Device Encryption**: Protects stored data (iOS auto-enables encryption with passcode).
- **External Media Encryption**: Encrypt removable storage (USB, SD cards).
- **Geofencing**: Trigger security actions based on location (disable camera in secure areas).
- **Restrict Sensors/Connections**:
  - Limit access to **camera**, **screen capture**, **Bluetooth**, **NFC**, **GPS**, etc.
  - Disable **tethering** and **hotspot** features if not needed.
- **Mobile Device Management (MDM)**:

- Enforce security policies, app controls, and remote wipe.
- Intune, JAMF, etc.

Connection & Location Controls

- **Wi-Fi**: Use secure enterprise networks; avoid public/rogue networks (evil twins).
- **Cellular/GPS**: Manage device tracking and data use.
- **PANs (Personal Area Networks)**: Bluetooth, wearables — restrict if not required.
- **NFC & Mobile Payments**: Secure short-range communication; disable if not needed.
- **VPNs**: Encrypt mobile traffic.

Lesson 11: Application Security

1. Secure Protocols

Insecure vs. Secure Protocols

Insecure Protocol	Secure Replacement	Purpose
Telnet	**SSH**	Secure remote shell access
HTTP	**HTTPS**	Secure web browsing
FTP	**SFTP / FTPS**	Secure file transfer

- **Insecure protocols** transmit data in **cleartext** (unencrypted).
- Always use **encrypted alternatives** to protect data in transit.

TLS (Transport Layer Security)

- **Use Only TLS 1.2 or 1.3**. Disable:
  - SSL 2.0 / 3.0
  - TLS 1.0 / 1.1
- **TLS 1.3** introduces **shortened cipher suites**, more secure and efficient:
  - Example: `TLS_AES_128_GCM_SHA256`
- Prevent **downgrade attacks** by enforcing minimum TLS versions.

Other Secure Services

- **LDAP** → Secure via LDAPS or StartTLS
- **SNMPv3**: Use only version 3 for encryption and authentication (v1/v2 are insecure)

---

2. Email Security

Anti-Spoofing & Integrity

Standard	Stands For	Function
SPF	Sender Policy Framework	DNS TXT record defines authorized mail servers
DKIM	DomainKeys Identified Mail	Digitally signs emails with sender's domain key
DMARC	Domain-based Message Authentication, Reporting & Conformance	Combines SPF/DKIM results to define how to handle failed email; adds reporting

Email Encryption

- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**:
  - Uses **PKI** (Public Key Infrastructure)
  - Provides **confidentiality, integrity**, and **authenticity** for email contents

Email Gateways

- Scan for:
  - **Spam**, **phishing**, **BEC (Business Email Compromise)** attacks
  - **Malicious URLs**, **harmful attachments**
  - Apply **URL Sanitization**, **Safe Linking**, etc.

Data Loss Prevention (DLP)

- Scans emails/attachments for:
  - **PII**, **PHI**, **payment data**, etc.
- Can:
  - Block, encrypt, or alert based on policy
  - Enforce compliance (GDPR,GLBA HIPAA, PCI DSS)

---

3. Secure Coding

Key Techniques

Technique	Purpose
Input Validation	Prevent injection (SQLi, XSS); validate length, type, format
Allow/Block Lists	Allow only safe data; block known bad input
Code Signing	Verify code integrity and source
Secure Cookies	Restrict cookies from being accessed via scripts or cross-site

Code Review Methods

- **Static Analysis**: Analyze source code without executing
- **Dynamic Analysis**: Run code to observe behavior
- **Peer Review**: Manual inspection by other developers

Dynamic analysis evaluates the software application in its running state and looks for vulnerabilities during its execution, which aligns with the analyst's requirement in the scenario.

Static code review evaluates the software's source code, bytecode, or application binaries without executing the software. While it is a valuable method, it does not meet the analyst's preference to assess the software while running.

Manual penetration testing involves actively probing for vulnerabilities in a running application, but it is broader than just analyzing the software's execution and can involve various techniques not limited to the software's runtime behavior.

Source code fingerprinting identifies software components and their versions by analyzing the software's source code.

Client-Side vs Server-Side Validation

Type	Secure?	Why?
Client-Side	❌	Can be bypassed by attackers
Server-Side	✅	Enforced regardless of user interface manipulation

---

4. Application Protections

- **Memory Management**:
  - Prevent **buffer overflows** via safe coding and validation
- **Error Handling**:
  - Avoid exposing sensitive info to users
  - Log internally, don't display full error details

Cloud Application Security

- Follows **Shared Responsibility Model**:
  - Cloud provider secures infrastructure
  - Customer secures application configuration and code

---

5. Software Sandboxing

- Isolates applications/processes from:
  - **Operating system**
  - **Other software**
  - **Network**
- Prevents malware from spreading or accessing system-level resources
- Often used in **malware detonation environments** (Joe Sandbox)

---

6. DNS Security

DNSSEC (DNS Security Extensions)

- **Prevents spoofing and cache poisoning**
- Adds cryptographic **validation** to DNS responses using signed records

DNS Filtering

Tool	Purpose
OpenDNS, Quad9, Pi-hole	Block access to known malicious or unwanted domains
DNS Filtering	Prevent access to malware, ads, or phishing sites

- Uses **blocklists, content categories**, and **real-time reputation** analysis

---

Key Differences Summary

Topic	Key Difference
SFTP vs FTPS	SFTP uses **SSH**, FTPS uses **TLS**
TLS 1.2 vs 1.3	TLS 1.3 uses **shorter, more efficient cipher suites**
SPF/DKIM/DMARC	SPF = who can send, DKIM = signed, DMARC = policy & reporting
Client-Side vs Server-Side Validation	Server-side is secure; client-side can be bypassed
HIDS vs Sandboxing	HIDS = detect threats; sandbox = isolate execution
DNSSEC vs DNS Filtering	DNSSEC validates responses; filtering blocks access

Lesson 12: Alerting and Monitoring

1. **Incident Response**
   - **NIST Phases**: Preparation to lessons learned.

1. Preparation

When to choose:

- Before an incident occurs.
- If the scenario describes setting up tools, policies, training, or incident response plans.

Example Scenario:

- "The company is updating its firewall rules and training employees on phishing awareness."

  ✅ **Correct Choice: Preparation**

---

2. Detection

When to choose:

- When the scenario mentions **identifying** or **noticing** a potential security issue.
- Key words: "alert," "unusual activity," "suspicious log entry," "IDS/IPS triggered."

Example Scenario:

- "An analyst receives an alert about multiple failed login attempts from an unknown IP."

  ✅ **Correct Choice: Detection**

---

3. Analysis

When to choose:

- When the scenario involves **investigating** the incident to understand its scope, impact, or cause.
- Key words: "determine the root cause," "assess the damage," "analyze logs."

Example Scenario:

- "The security team reviews logs to confirm if the suspicious activity is a breach."

  ✅ **Correct Choice: Analysis**

---

4. Containment

When to choose:

- When the scenario describes **stopping the spread** of the incident.
- Key words: "isolate the infected system," "block malicious IP," "disable compromised accounts."

Example Scenario:

- "The team disconnects an infected server from the network to prevent further damage."

  ✅ **Correct Choice: Containment**

---

5. Eradication

When to choose:

- When the scenario involves **removing the threat completely** (malware, attacker access).

- Key words: "delete malicious files," "patch vulnerabilities," "terminate attacker sessions."

Example Scenario:

- "The team removes a backdoor installed by hackers and patches the exploited vulnerability."

  ✅ **Correct Choice: Eradication**

---

6. Recovery

When to choose:

- When the scenario describes **restoring systems** to normal operations.
- Key words: "restore from backup," "reboot systems," "validate functionality."

Example Scenario:

- "The company brings its website back online after ensuring no malware remains."

  ✅ **Correct Choice: Recovery**

---

7. Lessons Learned

When to choose:

- After the incident is resolved, when the team **reviews what happened** to improve future response.
- Key words: "post-incident report," "improve policies," "update IR plan."

Example Scenario:

- "The security team holds a meeting to discuss how to prevent similar attacks in the future."

  ✅ **Correct Choice: Lessons Learned**

- **Forensics**: Chain of custody, disk imaging (dd).

Phase	When to Choose	Key Activities / Clues
1. Preparation	Before incidents occur	Create IR plans, set up tools, train staff, update security controls
2. Detection	When noticing or being alerted to an issue	Alerts, log anomalies, IDS/IPS triggers, user reports
3. Analysis	When investigating and assessing impact	Review logs, determine cause, assess damage and scope
4. Containment	To stop spread and limit damage	Isolate systems, block IPs, disable accounts, preserve evidence
5. Eradication	To remove threat completely	Delete malware, terminate sessions, patch systems
6. Recovery	To return systems to normal	Restore from backup, test systems, monitor
7. Lessons Learned	After incident is resolved	Post-incident review, update policies, generate reports

Supporting Concepts

- **Testing Types**:
  - **Tabletop**: Walkthrough, no live systems.
  - **Simulation**: Red team emulates attacker.
  - **Walkthrough**: Step-by-step response drill.
- **Threat Hunting**: Proactive detection of unknown threats using logs and intelligence data. Different from reactive incident response.

2. Digital Forensics

Due Process & Legal Hold

- **Forensics**: Preserve evidence for legal use.
- **Due Process**: Follow legal procedures and fairness.
- **Legal Hold**: Right to retain and seize digital assets.

Acquisition

- **Order of Volatility** (Capture most volatile first):
- When conducting a forensic analysis after an incident, it's essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.
  1. CPU registers, cache
  2. RAM
  3. Network data
  4. Disk
  5. Backups

- **Memory Acquisition**:
  - Live memory capture tools (Volatility Framework)
  - Collects RAM content, session keys, temporary files
- **Disk Imaging**:
  - **Live Acquisition**: While system is running
  - **Static Acquisition**: When system is shut down
  - Tools: `dd`, `dcfldd` (adds hashing and logging)

Preservation

- **Write Blockers**: Prevent data modification.
- **Hashing**: SHA256 for integrity (compare source vs image).
- **Chain of Custody**: Document each step from collection to court presentation.
- **Tamper Evidence**: Secure storage and bags.

Reporting

- **Summarize evidence and conclusions**.
- Must be **objective**, **repeatable**, and **non-tampered**.
- **E-discovery**: Process digital data (email, docs) for legal cases.

3. Data Sources

Common Data Sources

- **Memory & Disk**: RAM, file systems, metadata
- **Host Logs**: Security, system, app logs (Windows Event Viewer, syslog, journald)

- **Application Logs**: App-level activities, endpoint alerts
- **Network Logs**: Firewall, IDS/IPS (Suricata)
- **Packet Captures**: Full traffic visibility (Wireshark)
- **Metadata**: File timestamps, email headers, web request/response headers

Dashboards

- **Analyst View**: Alerts for triage.
- **Manager View**: Status and summaries.
- **Automated Reports**: For compliance and executive decision-making.

---

4. Alerting and Monitoring Tools

SIEM (Security Information and Event Management)

- **Log Collection**:
  - **Agent-Based**: Installed on endpoints
  - **Listener/Collector**: Listens to syslog/NetFlow
- **Aggregation**: Combine logs from various formats
- **Normalization**: Standardize fields
- **Time Sync**: Align timestamps across sources
- **Examples**: Splunk, Wazuh, Security Onion

Alerting and Correlation

- **Static Rules**: Trigger alerts on patterns or thresholds
- **Correlation**: Connect related events across sources
- **Threat Feeds**: Enrich alert context

Alert Tuning

Term	Meaning
False Positive	Alert triggered without actual threat
False Negative	Threat occurred but no alert triggered
True Positive	Correctly detected real threat

- **Tuning Techniques**:
  - Suppress noisy or redundant alerts
  - Adjust sensitivity
  - Redirect flood alerts
  - Use machine learning for pattern detection

---

5. Monitoring Infrastructure

Tool/Method	Purpose
SNMP Traps	Alert on hardware/software events
NetFlow/IPFIX	Monitor traffic flow statistics (who talks to whom, port/protocol)
Heartbeat Monitoring	Confirm system availability
Network Monitors	Track appliance and link state
System Logs	Detect uptime, usage, errors
Cloud Monitors	Detect cloud service outages

Vulnerability Scanners	Check for missing patches/config issues
DLP Tools	Detect and prevent sensitive data exfiltration

6. Benchmarks and SCAP

- **Security Content Automation Protocol (SCAP)**: NIST standard for automated compliance scanning
- **Used With**:
  - **OVAL** (Open Vulnerability and Assessment Language)
  - **XCCDF** (Extensible Configuration Checklist Description Format)
- **Purpose**: Detect misconfigurations, missing controls, or deviations from standards

Lesson 13: Analyze Indicators of Malicious Activity

1. Malware Attack Indicators

Malware is any software intentionally designed to cause damage to a computer, server, client, or network. Understanding the various **types**, their **behaviors**, and **signatures** is crucial for detecting and responding to malicious activity.

Viruses vs. Worms

- **Viruses** attach themselves to legitimate programs or files. They require user interaction to execute (like opening a file), and they typically spread through file sharing, email attachments, or USB drives.
- **Worms**, on the other hand, are self-replicating. They do not need a host file or user action to spread. They propagate through network vulnerabilities and can cause system slowdowns or crashes due to resource exhaustion.

> Security+ Key: Worms exploit system vulnerabilities and consume bandwidth, while viruses rely on user action and infected files.

Comparison: Virus vs. Worm

Feature	**Virus**	**Worm**
Needs Host File	Yes	No
Spreads via	Infected files, removable media	Network connections, remote vulnerabilities
Requires User Interaction	Yes	No
Primary Damage	Data corruption, file infection	Resource exhaustion, network congestion
Replication Speed	Slower (needs user)	Fast (automated replication)

Trojans vs. Potentially Unwanted Programs (PUPs/PUAs)

- **Trojans** are malicious programs disguised as legitimate applications. Once installed, they can open backdoors, steal credentials, or install other malware like keyloggers or RATs (Remote Access Trojans).
- **PUPs/PUAs** are applications that are installed without clear user consent. These include adware and bloatware. While not always malicious, they often degrade system performance, invade privacy, or serve as a gateway for more serious threats.

> Security+ Key: PUPs may come pre-installed or bundled; Trojans are intentionally malicious and hidden.

Comparison: Trojan vs. PUP/PUA

Feature	**Trojan**	**PUP/PUA**
Intent	Malicious	Not clearly malicious but unwanted
Delivery Method	Disguised as legitimate software	Bundled or silently installed with other applications
User Consent	Trickery (fake apps)	Often indirect or bundled in EULAs
Risk Level	High	Medium to Low
Common Payload	RATs, spyware, backdoors	Adware, toolbars, tracking software

Fileless Malware

Unlike traditional malware that writes files to disk, **fileless malware** operates entirely in memory, making it difficult to detect and analyze. It often uses legitimate tools like **PowerShell** or **WMI** to execute commands and maintain persistence through registry keys or scheduled tasks.

> Security+ Key: Detection is difficult with traditional antivirus; requires behavioral analysis and memory scanning.

Ransomware vs. Crypto-Malware

- **Ransomware** encrypts the victim’s data or locks access to systems, demanding a ransom for recovery. It may display a message screen or block system functionality entirely.
- **Crypto-Malware** focuses on hijacking system resources, especially CPU and GPU, to mine cryptocurrency like Monero, typically without the user's knowledge (this is called cryptojacking).

> Security+ Key: Ransomware is disruptive and demands payment. Crypto-malware is stealthy and aims to use resources over time.

Comparison: Ransomware vs. Crypto-Malware

Feature	**Ransomware**	**Crypto-Malware (Cryptojacking)**
Objective	Extort money by denying access	Exploit resources for cryptocurrency mining
Visibility	High (user is notified)	Low (runs in background silently)
System Impact	Loss of access to files/systems	Performance degradation, high CPU/GPU usage
Typical Delivery	Phishing, malicious attachments	Malicious scripts, ads, or trojans

Rootkits

A **rootkit** is a type of malware designed to gain and maintain privileged (root or SYSTEM) access to a computer while hiding its presence. It can replace core system files, hide processes, and purge logs to avoid detection. Rootkits may even reside in firmware or drivers.

> Security+ Key: Requires specialized tools to detect, such as boot-time scanners or kernel-level analysis.

Backdoors and Remote Access Trojans (RATs)

- **Backdoors** provide unauthorized access to a system and may be created intentionally by developers or inserted by malware.
- **Remote Access Trojans (RATs)** allow attackers full control of an infected system, often including screen viewing, file access, and remote shell.

> Security+ Key: RATs are types of Trojans that include remote control features. Backdoors may exist due to misconfiguration or malware.

Indicators of Compromise (IoCs)

IoCs are evidence that a system has been compromised. Examples include:

- Unusual outbound traffic
- New unknown processes or services
- High CPU usage
- Altered or missing logs
- Unexpected login attempts

> Security+ Key: IoCs are vital for forensic analysis and post-incident investigation.

---

2. Physical and Network Attack Indicators

Physical Attacks

Physical attacks target the environment or access control of the system. These include:

- **Brute Force Entry**: Physically breaking into server rooms.
- **Environmental Damage**: Tampering with HVAC or power systems.
- **RFID Cloning**: Copying data from proximity-based access cards.
- **Skimming**: Capturing data from card readers.

> Security+ Key: Physical security must complement cyber security (e.g., secure server cages, badge encryption).

DDoS Attacks (Distributed Denial of Service)

DDoS attacks overwhelm a target with traffic from multiple systems (botnets), causing downtime or service interruption.

Types of DDoS:

- **SYN Flood**: Exploits TCP handshake to consume resources.
- **Reflected**: Uses third-party servers to flood the target with replies.
- **Amplified**: Uses protocols like DNS/NTP to multiply traffic size.

Comparison: DDoS Types

Type	Description	Example Service Used
SYN Flood	Repeated spoofed TCP requests	Any TCP-based service

Reflected	Spoofs source IP to direct responses to victim	HTTP/DNS servers
Amplified	Sends small query, large response to victim	DNS, NTP, SNMP

On-Path (Man-in-the-Middle) Attacks

An attacker intercepts communication between two parties. Methods include:

- **ARP Poisoning**: Spoofs MAC addresses in a LAN.
- **DNS Spoofing**: Redirects users to malicious websites.

> Security+ Key: Use encryption (TLS), static ARP tables, and DNSSEC to mitigate.

Wireless Attacks

- **Evil Twin**: Fake AP mimics a real one to collect credentials.
- **Rogue AP**: Unauthorized AP used to gain access to network.
- **Rogue Access Point** is an unauthorized **wireless access point (WAP)** that has been connected to a **secure enterprise network** without the organization's knowledge or approval.
- **Deauthentication Attack**: Forces users off legitimate Wi-Fi.

Credential Attacks

These focus on stealing login information.

Types:

- **Brute Force**: Try all possible password combinations.
- **Password Spraying**: One password against many accounts.
- **Pass-the-Hash**: Uses NTLM hash instead of password.
- **Pass-the-Ticket**: Uses stolen Kerberos ticket.

Comparison: Credential Attacks

Type	Target	Method
Brute Force	Single account	Many passwords tried
Password Spraying	Multiple accounts	One password tested across users
Pass-the-Hash	Windows systems	NTLM hash replayed for authentication
Pass-the-Ticket	Kerberos environments	Uses Kerberos ticket for access

Cryptographic Attacks

- **Downgrade**: Forces systems to use older, weaker encryption.
- **Collision**: Two different inputs produce same hash.
- **Birthday Attack**: Probability-based collision attack.
- **Weak Cipher Exploits**: Attacks older algorithms like RC4, MD5.

> Security+ Key: Use TLS 1.3+, SHA-256 or better, and enforce forward secrecy.

3. Application Attack Indicators

Privilege Escalation

- **Vertical Escalation**: User gains higher privileges (e.g., admin).
- **Horizontal Escalation**: User gains access to another user's data.

Replay Attacks

These involve capturing and reusing valid authentication data like tokens or cookies to gain unauthorized access.

Forgery Attacks

- **CSRF (Cross-Site Request Forgery)**: Tricks user's browser into executing unwanted actions on authenticated sites.
- **SSRF (Server-Side Request Forgery)**: Forces a vulnerable server to send requests to internal systems or cloud metadata services.

Injection Attacks

Malicious code is injected into an application's input stream.

- **SQL Injection**: Alters SQL queries.
- **LDAP Injection**: Alters directory service queries.
- **XML External Entity (XXE)**: Exploits XML parsers to access files.
- **Command Injection**: Executes OS commands.

Directory Traversal vs. Command Injection

- **Directory Traversal**: Access unauthorized files using patterns like `../../../etc/passwd`.
- **Command Injection**: Executes shell commands via input fields.

Lesson 14: Security Governance Concepts

1. Policies, Standards, and Procedures

Policies:

- **Definition**: High-level rules that guide organizational behavior and decision-making.
- **Purpose**: Ensure compliance, define acceptable practices, and align teams with organizational goals.
- **Examples**:
  - **Acceptable Use Policy (AUP)**: Defines how employees can use company resources (no personal software on work devices).
  - **Incident Response Policy**: Outlines steps to handle security breaches (isolating infected systems).

Standards:

- **Definition**: Specific technical guidelines that support policies.
- standard defines the expected outcome of a task, such as a particular configuration state for a server or performance baseline for a service. Following the standard for each build would ensure each server's configuration would match.
- **Purpose**: Provide consistency and best practices for implementing policies.

- **Key Standards**:
  - **ISO 27000 Series**: International standards for information security management (ISO 27001 certifies an organization's security practices).
  - **NIST SP 800 Series**: U.S. federal guidelines (NIST SP 800-53 lists controls for securing government systems).
  - **PCI-DSS**: Payment Card Industry Data Security Standard. Protects credit card data (encrypting cardholder information).

Procedures:

- **Definition**: Step-by-step instructions for completing tasks.
- **Purpose**: Ensure tasks are performed consistently and compliantly.
- **Examples**:
  - **Onboarding**: Granting system access to new employees (creating user accounts).
  - **Patching**: Applying software updates (monthly Windows security updates).

Procedure	Description
Onboarding	The process of **setting up new users** within an organization, including account creation, assigning roles, providing access to systems, and initial training. Ensures users start securely and with appropriate permissions.
Offboarding	The process of **removing access** when an employee leaves the organization. Includes disabling user accounts, revoking credentials, collecting company-owned assets, and ensuring data is preserved or reassigned.
Background Checks	Conducting **pre-employment verification** such as criminal history, identity validation, and previous employment — to assess risk before granting access to systems or sensitive data.
Service Provisioning	Assigning and enabling **IT services** (e.g., email, cloud apps, VPN access) based on a user's role or department during onboarding. Helps align access with business need.
Software Provisioning	Installing or granting access to specific **applications** needed for the user's job, such as productivity software or specialized engineering tools. Often automated through group policies or deployment tools.
Desktop Deployment	Installing and configuring **endpoint devices** (laptops, desktops) for new users. Involves imaging systems, applying security configurations, and ensuring the device complies with organizational standards.
Patching & Updating	Ensuring that all new or existing systems have the **latest security patches and software updates** to reduce vulnerabilities from outdated software. Applies during onboarding and throughout employment.
Go-Live Actions	A checklist used when **deploying a new system or user** into production. Ensures all configurations, permissions, and dependencies are verified before the system or account goes active.
After-Hours Support	Defines the process for **handling support requests** or escalations outside of normal working hours, including who is on-call and how incidents are logged or prioritized.
Ticket Management	Guidelines for creating, updating, and resolving **help desk or security tickets**, ensuring that onboarding/offboarding actions are tracked, documented, and auditable.

Key Differences:

Concept	Policy	Standard	Procedure
Focus	*What* must be done	*How* to do it	*Steps* to complete a task
Flexibility	Broad and rigid	Detailed but adaptable	Specific and repeatable

Category	Policies	Standards	Procedures
Definition	Broad, high-level rules that define what must be done	Specific rules or guidelines that define how to meet policies	Detailed instructions that explain exactly how to perform a task step-by-step

Purpose	To set direction, expectations, and overall goals for the organization	To ensure uniformity and best practices when implementing policies	To provide a clear, repeatable way to complete specific tasks consistently
Scope	Organization-wide; applies to everyone	Department or system specific; supports policies with consistent practices	Task or role-specific; used by staff to carry out daily operations
Level of Detail	General and strategic – outlines *what* should be done	More technical – outlines *how* to do things consistently	Very specific – outlines *exactly how* to do something
Enforceability	Required and approved by senior leadership	Required to maintain compliance with policies	Required for operational consistency and legal/compliance requirements
Examples	- Acceptable Use Policy- Incident Response Policy	- ISO 27001 (security standard)- PCI-DSS (credit card security standard)	- Software patching steps- New employee account setup process

2. Legal and Regulatory Compliance

Global Laws:

- **GDPR (General Data Protection Regulation)**: **EU law protecting personal data** (requires consent for data collection).
- **CCPA (California Consumer Privacy Act)**: **Grants Californians rights over their data** (opt-out of data sales).

Industry-Specific Regulations:

- **HIPAA (Health Insurance Portability and Accountability Act)**: **Protects patient health data in the U.S. (encrypting medical records).**
- **FERPA (Family Educational Rights and Privacy Act)**: **Safeguards student records in U.S. schools (restricting access to grades)**.
- **PCI-DSS**: Mandates security for organizations **handling credit card transactions** (annual security audits).
- **GLBA (Gramm-Leach-Bliley Act)**: U.S. law requiring financial institutions to **protect consumer financial information** (implement safeguards for customer data and disclose privacy practices).

Privacy Laws

Law	Region	Purpose
GDPR (General Data Protection Regulation)	EU	**Protects personal data and privacy**; requires consent and transparency.
CCPA (California Consumer Privacy Act)	California, U.S.	**Grants Californians rights to access, delete, and opt-out of the sale of personal data.**

Energy Sector

Law	Region	Purpose
NERC (North American Electric Reliability Corporation)	U.S. & Canada	Enforces reliability standards for the bulk power system, including cybersecurity for energy infrastructure.

Education and Children

Law	Region	Purpose
FERPA (Family Educational Rights and Privacy Act)	U.S.	Protects the privacy of student education records.

CIPA (Children's Internet Protection Act)	U.S.	Requires schools/libraries to filter harmful online content to minors.
COPPA (Children's Online Privacy Protection Act)	U.S.	Restricts online data collection from children under 13.

Healthcare

Law	Region	Purpose
HIPAA (Health Insurance Portability and Accountability Act)	U.S.	Protects health information; requires safeguards for medical records and ePHI (electronic protected health information).

Financial Services

Law	Region	Purpose
GLBA (Gramm-Leach-Bliley Act)	U.S.	Requires financial institutions to safeguard consumer financial data and disclose information-sharing practices.
PCI-DSS (Payment Card Industry Data Security Standard)	Global (Contractual)	Enforces security for handling cardholder data (applies to any organization processing credit card transactions).

Government

Law	Region	Purpose
FISMA (Federal Information Security Modernization Act)	U.S.	Requires federal agencies to implement cybersecurity protections for **federal systems**.
CJIS (Criminal Justice Information Services Security Policy)	U.S.	Sets security requirements for systems that store or process criminal justice data.
GSC (The Government Security Classifications)	U.K	system for **classifying information** to protect it based on how sensitive it is

Consequences of Non-Compliance

Consequence	Description
Fines	GDPR fines up to €20 million or 4% of global revenue.
Legal Penalties	Civil or criminal lawsuits (HIPAA violations).
Loss of Contracts	For example, PCI-DSS non-compliance can result in loss of the ability to process credit cards.

3. Governance Roles

- **Data Owner**: Senior staff responsible for data classification (CFO owns financial data).
- **Data Controller**: is the person or organization that **decides why and how personal data is collected, used, and processed**
- **Data Processor**: is a person or organization that **processes personal data on behalf of the Data Controller**, but does NOT **decide why** or **how** the data is **used**. They follow the controller's instructions. (a cloud storage provider).
- **Data Custodian**: Manages data storage and security (IT department encrypting files).
- Data Subject: is the individual whose personal information is collected, processed, or stored by an organization.

4. Change Management

Process:

1. **Propose Change**: Submit a request (upgrading server hardware).
2. **Review by Change Board**: Assess risks and impacts (downtime during upgrade).
3. **Test**: Validate changes in a sandbox environment.
4. **Implement**: Deploy changes during maintenance windows.

5. **Backout Plan**: Revert changes if issues arise. (snapshot can be a part of a backout plan just for a example but the snapshot more technical tool than detailed procedure)

Allow Lists vs. Deny Lists:

- **Allow List**: Pre-approved items (only Microsoft Teams can be installed).
- **Deny List**: Blocked items (banning peer-to-peer software like BitTorrent).

Documentation:

- **Version Control**: Track changes to policies (using Git for code updates: GitHub, Gitlab).
- **Legacy Systems**: Older systems needing special handling (compatibility testing for Windows 7).

---

5. Automation and Orchestration

Automation:

- **Definition**: Using scripts/tools to perform tasks without manual effort.
- **Examples**:
  - **Scripting**: PowerShell scripts to deploy patches.
  - **Security Automation**: Blocking malicious IPs detected by firewalls.

Orchestration:

- **Definition**: Coordinating automated tasks across systems.
- **Example**: Deploying updates to 100 servers simultaneously using Ansible.

Challenges:

- **Complexity**: Requires skilled staff to design workflows.
- **Technical Debt**: Poorly maintained scripts can create security gaps.

Lesson 15: Risk Management Processes

1. Risk Identification and Assessment

Risk Identification:

- **Definition**: The process of pinpointing potential threats to an organization (malware, phishing, insider threats, equipment failures).
- **Examples**:
  - **Technical Risks**: Software vulnerabilities, network breaches.
  - **Nontechnical Risks**: Poor employee training, outdated policies.

Risk Analysis:

- **Quantitative Analysis**:
  - **Definition**: Uses numerical values to calculate risk (financial loss).
  - **Key Metrics**:

- **Single Loss Expectancy (SLE)**: Cost of one incident ($10,000).
- **Annual Rate of Occurrence (ARO)**: Number of times a risk occurs yearly (2 times).
- **Annualized Loss Expectancy (ALE)**: SLE × ARO ($20,000).

Term	Key Difference
SLE	Measures **cost per single incident**
ARO	Measures **how often** the incident occurs per year
ALE	Measures **total yearly loss** (calculated as SLE × ARO)

Each **incident type** (or risk scenario) has its **own SLE, ARO, and therefore its own ALE**

Incident Type	SLE	ARO	ALE
Data breach	$50,000	1	$50,000
Ransomware infection	$10,000	3	$30,000
Lost company laptop	$2,000	5	$10,000

- **Qualitative Analysis**:
  - **Definition**: Uses subjective judgment to prioritize risks ("high," "medium," "low").
  - **Tools**:
    - **Heat Maps**: Visual grids ("traffic light" charts) to rank risks by likelihood and impact.

Key Terms:

- **Inherent Risk**: Risk level before applying controls.
- **Residual Risk**: Risk remaining after mitigation (after implementing firewalls).

---

2. Risk Management Strategies

Risk Responses:

1. **Avoid**: Eliminate the risk (discontinuing a vulnerable service).
2. **Accept**: Acknowledge the risk without action (low-impact risks), This minor web vulnerability only costs $500 if exploited — we'll accept it."
3. **Mitigate**: Reduce risk impact (installing antivirus software).
4. **Transfer**: Shift risk to a third party (purchasing cyber insurance).

Risk Appetite:

- **Definition**: The level of risk an organization is willing to tolerate ("No high-risk vulnerabilities allowed").
- "We are okay with up to $50,000 in annual cyber losses."
- **High Risk Appetite** → Low and Medium risks are often **accepted**.
- **Low Risk Appetite** → Even small risks might **require action**.

Differences:

Term	Definition	Key Focus	Example
Risk Appetite	The **general level of risk** an organization is **willing to**	High-level, strategic view	A company may accept **moderate risks** to pursue innovative

	accept to achieve its goals.		technologies.
Risk Tolerance	The **specific range or degree of variation** from the risk appetite that is acceptable.	Operational boundaries around appetite	A system can tolerate **up to 5 hours** of downtime in a year.
Risk Threshold	The **quantitative point** at which risk becomes **unacceptable** and triggers action.	Action trigger point	If expected downtime exceeds **5 hours**, mitigation must occur.

Think of it like driving:

- **Risk Appetite:** "I'm comfortable driving up to 80 mph." (strategic comfort level)
- **Risk Tolerance:** "But I prefer staying between 60–75 mph." (acceptable range)
- **Risk Threshold:** "If I hit 76 mph or more, I'll slow down immediately." (action line)

---

3. Risk Management Processes

Risk Register:

- **Definition**: A document listing identified risks, their severity, owners, and mitigation plans.
- **Example**:

Risk	Severity	Owner	Mitigation
Phishing Attacks	High	IT Team	Employee training, email filters

Key Risk Indicators (KRIs):

- **Definition**: **Metrics predicting potential risks (increased failed login attempts)**.

Risk Reporting:

- **Purpose**: Communicate risk status to stakeholders (quarterly risk reports).

---

4. Business Impact Analysis (BIA)

Key Metrics:

- **MTD (Maximum Tolerable Downtime)**: Longest time a system can be offline (4 hours for payment processing).
- **RTO (Recovery Time Objective)**: Time to restore systems after a disaster (2 hours).
- **RPO (Recovery Point Objective)**: Maximum data loss acceptable (1 hour of data).
- **WRT (Work Recovery Time)**: Time to restore workflows (3 hours to resume operations).

Term	Key Difference	Meaning	Example
MTD (Maximum Tolerable Downtime)	**Total max downtime allowed** before major impact	Full time from outage to full operation (includes all recovery phases)	Business can survive **up to 6 hours** of downtime before serious loss
RTO (Recovery Time Objective)	**Time to restore systems** after disaster	How fast you can get systems (servers, apps) running again	Systems **must be restored in 2 hours** to meet SLA
RPO (Recovery Point Objective)	**Max acceptable data loss** (in time)	How recent the last backup needs to be	Acceptable to lose **no more than 30 minutes** of data
WRT (Work Recovery Time)	**Time to restore workflows** after systems are up	Time needed for people/processes to resume work (manual checks, reconfig, etc.)	After systems are restored, **1 hour is needed** to re-enter transactions

5. Vendor Management Concepts

Vendor Selection

Selecting the right vendors is a critical part of maintaining a strong security posture and minimizing third-party risk. This process involves systematically evaluating and assessing vendors during procurement or outsourcing.

- **Third-Party Vendor Assessment**:
  - A key element of Governance, Risk, and Compliance (GRC).
  - Helps provide documented evidence of due diligence.
  - Due diligence: The process of **carefully researching, evaluating, and verifying** the security, legal, financial, or operational aspects of a vendor, partner, system, or investment **before committing** to it.

    Due diligence Example:

    Before hiring a cloud storage provider, your security team:

    - Reviews their breach history.
    - Checks their data encryption and access control policies.
    - Confirms they meet regulations like GDPR or HIPAA.

- **Conflict of Interest**:
  - Occurs when an individual or vendor has competing interests (a vendor holds financial interest in a competitor).
  - Can compromise objectivity and introduce bias or risk.
- **Vendor Assessment Methods**:
  - **Evidence of Internal Audits**: Vendors should demonstrate internal control checks.
  - **Independent Assessments**: External audits by third parties.
  - **Penetration Testing**: Ethical hacking to uncover security weaknesses in vendor environments.
  - **Supply Chain Analysis**: Evaluate upstream/downstream risks related to vendor partners.
  - **Right-to-Audit Clause**: Allows organizations to audit a vendor's systems, processes, or controls.
- **Vendor Monitoring**:
  - Continuous evaluation of vendors to ensure they remain compliant with security policies, service-level expectations, and legal agreements.

Legal Agreements

Organizations should establish formal agreements with vendors to clarify expectations, obligations, and rights. These may be categorized into **initial agreements** and **performance/operational agreements**.

- **Initial Agreements**:
  - **Memorandum of Understanding (MOU)**: Informal, non-legally binding agreement outlining mutual intentions.
  - **Memorandum of Agreement (MOA)**: More formal than an MOU, detailing responsibilities; may be legally binding.
  - **Nondisclosure Agreement (NDA)**: Prevents parties from sharing confidential information.
  - **Business Partnership Agreement (BPA)**: Governs how business partners work together (profit sharing, responsibilities).
  - **Master Service Agreement (MSA)**: Broad agreement setting overall terms for long-term vendor relationships.

Agreement	Key Difference
MOU (Memorandum of Understanding)	Informal, not legally binding
MOA (Memorandum of Agreement)	More formal than MOU; can be legally binding (By lawyers)
NDA (Nondisclosure Agreement)	Protects confidential information from being shared
BPA (Business Partnership Agreement)	Defines how business partners operate together
MSA (Master Service Agreement)	Sets general terms for ongoing vendor services

- **Operational / Performance Agreements**:
  - **Service-Level Agreement (SLA)**: Specifies **performance** expectations, such as uptime (99.9% availability), response times, and penalties for non-compliance.
  - **Statement of Work (SOW) / Work Order (WO)**: Details specific tasks, deliverables, timelines, and costs under the umbrella of a broader agreement like an MSA.

Agreement	Key Difference	Clear, Realistic Examples
SLA (Service-Level Agreement)	Sets **performance and uptime expectations**; includes metrics, penalties, and support terms	- Cloud provider guarantees **99.9% uptime** for hosting services - Helpdesk must **respond to critical tickets within 30 minutes** - Backup service must **complete daily backups by 2:00 AM** - Provider pays **10% monthly credit** if response time exceeds SLA
SOW / WO (Statement of Work / Work Order)	Lists **exact deliverables**, timeline, cost, and responsibilities for a specific project	- Vendor must **deploy 50 new laptops** with security baselines in 10 business days - Consultant will **audit 3 remote sites** and deliver a report by **June 15** - Pen tester will **conduct a black-box test** on the web app and submit findings in 5 days - Contractor will **migrate on-prem servers to Azure**, budget capped at $15,000

- **Expectations**:
  - **Rules of Engagement (RoE)**: Especially relevant for security testing; defines scope, boundaries, and permissions (for penetration testing) to avoid legal or operational issues.

---

6. Audits and Assessments

Attestation and Assessments

- **Attestation**:
  - A formal process that **verifies the accuracy, reliability, and effectiveness** of implemented security controls.
  - May be conducted by internal staff or external auditors depending on the need.

- **Internal Assessment**:
  - Conducted by the organization's own employees.
  - Often **customizable**, easier to schedule, and used for regular internal review.
  - Example: Quarterly security audits or policy compliance checks.
- **External Assessment**:
  - Performed by **independent third parties**.
  - External experts or consultants conduct an external assessment to evaluate an organization's overall performance, practices, capabilities, or specific focus areas.
  - Provides **unbiased and objective evaluations**.
  - Often required for **legal compliance** (ISO 27001, SOC 2).

Internal vs. External Audits

- **Internal Audit**:
  - Done by internal teams (security or compliance departments).
  - Focuses on internal controls, policy compliance, and risk management.
  - Example: Internal audit of employee access controls.
- **External Audit**:
  - Conducted by third-party organizations.
  - Often part of **certification or regulatory processes**.
  - Example: External audit for PCI-DSS or ISO 27001 certification.

Penetration Testing (Pen Test / Ethical Hacking)

- **Purpose**:
  - Uses authorized hacking techniques to identify **exploitable weaknesses** in systems, networks, or applications.
  - May involve **active** (hands-on testing) and **passive** (observation) reconnaissance.
- **Test Types by Environment**:
  - **Known Environment (White Box)**: Testers have full access and system knowledge.
  - **Partially Known Environment (Gray Box)**: Testers have limited insight or partial access.
  - **Unknown Environment (Black Box)**: Testers act like external attackers with no internal knowledge.
- **Penetration Testing Types**:
  - **Internal Penetration Testing**: Focuses on threats from inside the organization.
  - **Physical Penetration Testing**: Tests physical security, such as access to buildings or server rooms.
  - **Integrated Penetration Testing**: Combines multiple types (network + physical + social engineering).

Exercise Teams

- **Red Team**:
  - Offensive team that simulates real-world attacks.
  - Identifies vulnerabilities and tests defenses.
- **Blue Team**:
  - Defensive team that detects and responds to attacks.
  - Focuses on protecting systems and monitoring responses.

Key Standards and Frameworks

- **NIST SP 800-37**: Guides organizations through risk management steps (Identify, Assess, Respond, Monitor).
- **ISO 31000**: International standard for risk management best practices.
- **MITRE ATT&CK**: Framework mapping adversary tactics for penetration testing.

Lesson 16: Data Protection and Compliance Concepts

1. Data Classification

Definition: Categorizing data based on sensitivity and required protections.

Key Types:

- **Regulated Data**: Legally protected (PII, PHI, financial records).

Term	Key Difference	Meaning
PII (Personally Identifiable Information)	Identifies an individual directly or indirectly	Any data that can be used to identify a person (name, SSN, email, address, date of birth)
PHI (Protected Health Information)	Health-related PII regulated under HIPAA	Medical data linked to a person (diagnoses, treatment history, lab results, insurance info)
Financial Records	Data related to financial transactions or account details	Includes banking info, credit card numbers, tax returns, income statements, credit reports

- **Trade Secrets**: Proprietary business information (Coca-Cola recipe).
- **Intellectual Property**: Copyrights, patents, trademarks.
- **Legal/Financial Data**: Contracts, tax records, audit reports.

Classification Levels:

1. **Public**: Non-sensitive (marketing materials).
2. **Confidential**: Requires restricted access (employee records).
3. **Private**: Highly sensitive (encryption keys, trade secrets).
4. **Privacy**: Personal data requiring protection to maintain individual rights (PII, PHI, financial records).

Term	Key Difference	Meaning	Examples
Public	Least sensitive, freely shareable	Data intended for public consumption; no security needed	Marketing content, website text, press releases
Confidential	Internal-use only, moderate sensitivity	Info that could harm the org if exposed; access limited to authorized staff	Internal policies, employee schedules, project docs
Private	Highly sensitive, tightly restricted	Information critical to business operations; breach could be damaging	Trade secrets, encryption keys, intellectual property
Privacy	Protects individual identity and rights	Any data that can identify a person; requires legal protection	PII (names, SSNs), PHI (medical history), bank records

Example:

- Microsoft Azure uses labels like **Confidential** to auto-apply watermarks and restrict document access.

---

2. Data Sovereignty and Geographical Considerations

Data Sovereignty:

- **Definition**: Laws requiring data to be stored and processed within a country's borders (GDPR mandates EU data stays in the EU).

  Different countries have different **privacy laws**, **government access rules**, and **security regulations**.

  If your company stores data in another country (like using a cloud server in the US while you operate in Germany), the data could be:

  - Accessed by foreign governments (under their local laws),
  - Not compliant with your country's data protection laws.

Geographical Considerations:

- **Access Controls**: Verify user locations (geo-blocking).
- **Example**: A Canadian bank must store customer data on servers within Canada.

Key Regulations:

- **GDPR** (EU): Protects EU residents' data globally.
- **CCPA** (California): Grants Californians rights over their data.

---

3. Privacy Data

Definition: Information tied to an individual's identity (Social Security numbers, medical records).

Key Concepts:

- **Right to Be Forgotten**: GDPR allows individuals to request data deletion.
- **Data Inventories**: Track where personal data is stored (CRM systems).
- **Data Retention**: Keep data only as long as necessary (delete old customer records after 7 years).

Roles:

- **Data Controller**: Decides how data is used (a company collecting emails).
- **Data Processor**: Handles data on the controller's behalf (cloud providers like AWS).

---

4. Privacy Breaches and Data Breaches

Breach Types:

- **Privacy Breach**: Unauthorized access to personal data (leaked patient records).
- **Data Breach**: Any unauthorized access to data (stolen credit card numbers).

Consequences:

- **Fines**: GDPR fines up to €20 million or 4% of global revenue.
- **Notifications**: GDPR requires breaches to be reported within 72 hours.

---

5. Compliance

Definition: Adhering to laws, regulations, and contractual obligations.

Key Issues:

- **Legal Noncompliance**: Violating GDPR, HIPAA, or PCI-DSS.
- **Software Licensing**: Using unlicensed software (pirated Microsoft Office).

- **Contractual Noncompliance**: Failing to meet SLA terms (uptime guarantees).

Monitoring:

- **Internal Audits**: Regular checks by the organization.
- **External Audits**: Third-party reviews for certifications (ISO 27001).

---

6. Data Protection Methods

Data States:

- **At Rest**: Stored data (encrypted databases).
- **In Motion/transit**: Data being transmitted (HTTPS for web traffic).
- **In Use**: Data being processed (RAM encryption).

State	Encryption Method / Protective Technology
Data At Rest	Full Disk Encryption (FDE), File-level Encryption, Database Encryption, BitLocker, LUKS
Data In Transit	TLS/SSL, VPN, SSH, IPSec, HTTPS, Secure FTP (SFTP), Encrypted Messaging Protocols
Data In Use	Trusted Execution Environment (TEE), Homomorphic Encryption, Secure Multiparty Computation (SMPC), RAM encryption, Intel SGX, AMD SEV

Homomorphic: encryption allows data to be encrypted and manipulated without needing to decrypt it first

Data Loss Prevention (DLP)
:

- **Definition**: Tools that block unauthorized data transfers (preventing emailing of credit card numbers).
- **Example**: Office 365 DLP policies flag sensitive files shared externally.

---

7. Personnel Policies

Conduct Policies:

- **Acceptable Use Policy (AUP)**: Rules for using company resources (no torrenting).
- **Clean Desk Policy**: Employees must secure sensitive documents before leaving.
- **Social Media Use**: Guidelines for posting company information online.

Training:

- **Role-Based Training**:
  - **End Users**: Spot phishing emails.
  - **IT Staff**: Secure network configurations.
- **Techniques**:
  - **Phishing Simulations**: Test employee vigilance.
  - **Gamification**: Reward employees for completing training modules.

Security Awareness Lifecycle:

1. **Assessment**: Identify training needs.
2. **Planning**: Design tailored programs.
3. **Delivery**: Conduct workshops/CBT.

4. **Evaluation**: Measure effectiveness via quizzes.

مع تمنياتي لكم بالنجاح

> **Qays Sarayra**
>
> **Read & Approved by Mustafa Hajeir + Osama Ismail**