DAY-4

(Access Control and Identity Management).

1.) Introduction to IAM (Identity and Access Management).

→ IAM is a framework of policies, processes, and technologies that manage digital identities and control access to resources in an organization. It ensures the right users have the right access to the right resources at the right time.

→ Purpose :- ⊙ Security :- Protects sensitive data and system from an unauthorized access.

⊙ Compliance :- Meets regulatory requirements (eg-> GDPR, HIPAA).

⊙ Efficiency :- Streamlines user access and reduces administrative overhead.

IAM Components :-

⊙ Identity Management : (creating, managing, and deleting user identities (eg :- user accounts, profiles).

eg> User provisioning in Active Directory (AD) to assign usernames and passwords

No.
Date

① Authentication : Verifying a user's identity (eg → entering a password or using biometrics).

② Authorization : Determining what is verified user can do (eg) read only vs admin access).

③ Auditing / Reporting :- Tracking access activities for accountability (eg → login logs).

2. AAA Model :-

AAA is (Authentication, Authorization, Accounting) a security framework for controlling access and tracking user activities.

1.) Authentication :- (Definition ✓)
- Methods → Password, biometric, tokens
- ② Common Protocols → LDAP, RADIUS

eg) Logging into VPN with a user name and password.

2.) Authorization :- (Definition ✓)

eg) A user can access a shared folder but not modify it.

④ Tools ⇒ ACLs, RBAC.

3. Accounting ⇒ Definition (✓)

eg) Logging who accessed a server and when.

Tools → SIEM system like Splunk, or syslog for log collection

3. Access Control Models :-

① DAC (Discretionary Access Control) :
→ Resource owners decide who gets access.
→ Characteristics :- Flexible, user-driven, less secure for sensitive systems.
eg) Sharing a Google Drive folder with specific users.
→ Pro's → Easy to manage for small system
→ Con's → Risk for over-permission or misconfig.

② MAC (Mandatory Access Control) :-
→ Access is controlled by a central authority based on security levels (eg → Classified, secret).
→ Characteristics :- Strict, used in high-security environments. (eg → govt).
Example → A soldier with secret cannot access 'Top Secret' files.
→ Pro's → High security, strict policies
→ Con's → Complex, less flexible.

3.) RBAC (Role-Based Access Control):-
→ Access is granted based on user roles (eg→ admin, employee).
• Character → Scalable, widely used in company
• Eg → A payroll manager can access payroll system but not IT admin tools.
• Pro → reduce risk, Simplifies managment
• Cons → Role creep.

4) ABAC : (Attribute-Based access control)
→ Access is granted on attributes (eg→ user location, device, time).
→ Characteristics → Dynamic, Context-aware, complex to implement.

eg→ Allowing access to a file only if user is in the office and using company device.

• Pro → Highly granular and flexible.
- Cons → Requires robust attribute management.

PTO.

4.) Multi-Factor Authentication (MFA).

MFA requires two or more verification factors to authenticate a user, ↑ security

Types (Factors):-

① Something You Known :→ Password, PIN, Questio
② Something ↓ Have : Phone (for OTP), card.
③ ↓ ↓ Are : Biometrics.

Real-World Use :-
• Banking : logging into online banking with a password and then OTP.
⊙ Work place → accessed by (fingerprint + passwor
⊙ Challenges →
User inconvenience, Costly.

5.) Principle of Least Privilege :-
Users or system should have the minimum access necessary to perform their tasks.

Importance
⊙ Reduce risk :- Limits damage from compromised accounts (eg→ hacked user can't access admin function).
⊙ Compliance :- Required by standards like PCI DSS & ISO 27001.

Example :- If junias can monitor system but not install software.

Implementation :->
- Regular access reviews to remove unnecessary permissions.
- Use RBAC to assign permission.

6.] Security Controls :-
Mechanisms to protect systems by preventing, detecting or responding to threat.

Types :-
1) Preventive :-> Stops threats before they occur. (eg-> Firewalls, MFA)
2) Detective :-> Identifies threats during or after an incident. (eg-> IDS/IPS, SIEM, antivirus)
3) Corrective : Mitigates damage after an incident. (eg-> Backups, Patch management, Incident response plans).
4) Compensating :- Alternative controls, when primary one fails. (eg-> Requiring Manager approval for sensitive access if MFA isn't available).

7.] Physical Security Basics :-
Physical security protects hardware, facilities and personnel from unauthorized access or damage.
eg->
- CCTV :- Monitors premises for suspicious activity.
- Access Cards :- Restrict entry to secure areas (eg-> Server rooms).
- Locks :-> Secure devices and physical assets. (eg-> laptop lock)
- Biometric Scanners => Uses fingerprints or iris scans for entry.

Importance ->
1) Prevent theft of devices containing sensitive data.
2) Complements Digital security (Digital + Physical security => 0G).

PTO.

No.

Date

8.) Authentication Mechanisms :-

(1) Password Policies :-

Rules to ensure strong passwords (eg→ minimum length, complexity).

- Best Practices

  - At least 12 characters, mix of letters, no., symbol
  - Avoid reuse across systems.
  - Enforce regular password changes (eg→ after 90 days).

eg→ A policy requiring passwords like 'P@ssw0rd!2025' instead of 'Password123'.

(2) Token - Based Access :-

- One-Time Password : Temporary codes sent via SMS, email, authenticator app.
- Smartcards :- Physical card with chip for authentication (eg CAC cards in govt).

eg→ Logging into VPN with password and an OTP from a mobile app.

No.

Date

⊙ HTTPS Downgrade Attacks :

→ Attackers force a connection to use HTTP instead of HTTPS to intercept data.

→ Prevention :-

① Enable HSTS to enforce HTTPS

② Use secure cookies and redirect HTTP to HTTPS

eg: A Hacker uses a rogue WiFi hotspot to downgrade a user's banking session to HTTP.

Additional Topic : (System Maintenance)

1) Patching.
2) Config Management.
3) Backup & Recovery.
4) System Hardening.
5) Monitoring & Auditing.
6) Lifecycle Maintenance.

Created lvl → 8.5/10) for cybersec.

No.

Date

[DAY-4B] (Threat Intelligence + GRC).

1) Threat Intelligence + GRC Laws :-

- What is Threat Intelligence?

→ TI (Threat Intelligence) is actionable information about potential or current cyber threats, such as malware, phishing campaigns, or APTs, gathered to preempt or mitigate attacks. It transforms raw data into insights that help organization prioritize defenses.

- Sources :- Open-source intelligence (OSINT) from public data (eg → blogs, forums), commercial feeds from vendors (eg → FireEye), and internal data from logs or incident reports.

- Types :- ① Strategic TI, ② Tactical TI, ③ Operational TI, ④ Technical TI.

① Strategic TI :- High-level, long-term insights into threat trends and geopolitical factors
Eg → A report predicting a rise in ransomware due to economic instability, aiding C-level decision-making on budget allocation.

② Tactical TI :- Focuses on specific techniques and tools used by attackers

(eg, Phishing email templates or exploit kits)
• Useful for security teams to update defense like email filters.

③ Operational TI :- Detailed, near-real-time data about imminent threats, such as an APT targeting a sector. Includes indicators like IP addresses or malware signatures for immediate response.

④ Technical TI :- Granular data for IT teams, like vulnerability exploit details or malicious code samples, often shared via STIX/TAXII formats for automated integration into security tools.

5 Application :- TI with assets to prioritize patching or deploy counter measures (eg: blocking IPs).

GRC & GRC Laws Overview :-

① Definition of GRC :⇒ GRC stands for Governance, Risk, and Compliance. It is a strategic framework that integrates these core components to manage an organization's cybersecurity posture, align it with business objectives, and ensure adherence to legal and regulatory requirements.

• Governance :- The system of policies, roles and processes that guide and oversee security practices to align with organizational goals.

• Risk :⇒ Done before.

• Compliance :- The practice of meeting external laws, regulations, and internal policies to avoid penalties and maintain trust.

② Purpose :⇒ GRC provides a unified approach to manage cyber risks, ensure regulatory adherence (eg: GDPR), and foster a culture of accountability. It helps organizations respond to evolving threats like ransomware or data breaches proactively.

• Core components of GRC :-

1) Governance :⇒

Key elements ⇒ ① Policies : Written rules

(eg→ Acceptable Use Policy) defining security expectations.

- Roles & Responsibilities → Assigns duties (eg→ Chief Info Security Officer oversees strategy, IT teams implement controls).

- Decision-Making Processes :- Ensures transparent approval of security initiatives.

▲ Implementation :-

- Develop a cybersecurity policy framework, including data classification and access control guidelines.
- Conduct regular governance review to adapt to new threats or business changes.

① Risk :- (All done) just some extra stuff

-Tools :- Risk assesment framework (eg→ NIST SP 800-30), Software (eg→ Risk Watch).

① Intermediate Insight :- Risk management uses metrics like Annual Loss Expectancy (ALE = Single loss expectancy x annual rate of occurance) to quantify impact.

② Compliance :- (compliance ensures an organization meets external regulations, industry standards and internal policies.

▲ Types

① External :- Adherence to laws (GDPR) and Standards (eg→ PCI DSS).

② Internal :- Following company-specific policies (eg→ Password standards).

▲ Activities :-

① Conduct audits to verify adherence
② Document compliance evidence (eg→ log files, policy acknowledgments).
③ Train employees on regulatory requirements.

GRC Frameworks and standards :-

⊙ Purpose : Frameworks provide structured guidelines to implement GRC effectively.

Frameworks :-

- NIST Cybersecurity Framework :

Function → Identify, Protect, Detect, Respond, Recover., Used by USA organization.

- Application → Helps access current security posture and plan improvements (eg → Detect uses intrusion detection system).

⊙ Identify → Asset managment (eg → inventory servers), risk assesment (eg → Vulnerability scans).

⊙ Protect → Access control (eg → MFA), awareness training, data security : (eg → Encryption).

⊙ Detect :→ Continuous monitoring (eg → IDS), anomaly detection (eg SIEM alert).

⊙ Recover, Respond → Restoration (eg → backups), Improvement (eg → Post-incident review).

⊙ Respond → Response planning, communications, miligation (eg → isolate infected systems).

- Tiers → Partial (Tier 1) to Adaptive (Tier 4) maturity levels, guiding implementation.

- Use → A retailer uses NIST to recover from a DDoS by restoring services and updating firewalls.

ISO 27001 :-

→ Based on Annex A with 114 controls across 14 domains (eg → A.5 Information security Policies, A.12 · Operation Security).

→ It is international standard for information security Managment System (ISMS).

→ Requires risk assessments, Security controls, and audits.

→ Certification process ensures compliance.

No.
Date

- Process → Risk assessment → ISMS design → Implementation → Monitoring → Certification audit.

- Controls → Include encryption (A.13.2), access control (A.9) and incident management (A.16).

- Certification → Third-party audits ensure compliance, renewable every three to years.

Use → A bank implements ISO27001 to secure customer data, passing an audit with documented control.

COSO Framework :-

→ Focuses on enterprise risk management, integrating with GRC to enhance internal control.

→ Intermediate Detail → Links to financial reporting (eg → Sarbanes-Oxley Act [SOX]) and operational resilience

GRC Laws and Regulations :-

1. Overview → GRC laws are legal mandates organization must follow, enforced by governmental or industry bodies, with penalties for non-compliance.

- Key GRC Laws :-

1. GDPR (General Data Protection Regulation) →

- Scope : Applies to EU residents' data, globally if processed by EU-linked entities

- Requirements : Data breach notification within 72 hours, user rights (eg → data portability), fines upto to €20mn or 4% annual turnover.

- Relevance :- Impacts data handling (eg → encryption mandates).

2. HIPAA (Health Insurance Portability and Accountability Act) :-

- Scope → US law for healthcare providers and associate.

audits; penalties include jail time for executives.

- Relevance Links GRC to financial cybersecurity

4) PCI DSS (Payment Card Industry Data Security Standard):

- Scope → Mandatory for entities handling Cardholder data.
- Requirements → 12 requirements (eg → access control, encryption. Updated to v4 in 2022 with MFA emphasis
- Relevance → Protects Payment transaction

5. (Implementing GRC in Cybersecurity):-

- Steps:-

(a) Assess Current State: Conduct a gap analysis to identify weaknesses in governance, risk or compliance.

No.

Date

• Solutions :-

① Use integrated GRC platforms (eg → IBM open pages) for centralized management.

② Outsource to Managed Security Services Providers (MSSPS) for expertise.

③ Adopt automation (eg → AI driven risk assessments).

▲ Benefits and Challeges of GRC :-

→ Benefits :-

- Risk Reduction :- Identifies vulnerabilities early (eg → unpatched system).
- Compliance Assurance : Avoids fines (eg → GDPR penalties average 1mn$)

① Efficiency → Streamlines processes, reducing audits.

② Reputation :- Builds customer trust through transparent security practices.

→ Challeges :- ① Complexity ↑ : Highly complex

② Costly : ↑ Highly costly.

③ Resistance : → Employee may resist new policies.

Practical Applications and key activities :-

Scenarios :-

① Healthcare : Use HIPAA-aligned GRC to secure patient records with encryption and audits.

② E-commerce : Implement PCI DSS for Payment security, using GRC to monitor compliance.

Key Activities :-

① Conduct risk assessment for a hypothetical company, listing 5 risks and mitigation strategies.

② Draft a basic governance policy for remote work, including VPN and MFA requirements.

③ Map GDPR requirements to a company's data handling process, identifying compliance gaps.

Security Policies and Procedure :-

Security Policies :- Formal, high level documents that establish rules and guidelines to protect an organization's information assets, system and data from threats. They define the 'What' and 'why' of security practices.

Security Procedure :- Security procedures are detailed, step-by-step instruction that operationalize policies, specifying the 'How' to implement security measures effectively and consistently.

- **Purpose in CyberSecurity :-**
  - Together, they ensure a structured approach to safeguarding assets, reducing risks and meeting compliance requirements. They serve as a foundation for employee behaviour, incident response, and audits.

Core Components of Security Policies :-

① Acceptable Use Policy (AUP) :-

:- Outlines permissible use of IT resources (eg → no personal use of company laptops).

→ Key elements :- Prohibitions (eg → downloading unauthorized software); Consequences (eg → disciplinary action), and user acknowledgment.

② Password Policy → Already done

③ Incident Response Policy :-

→ Defines the process for identifying, managing, and recovering from security incidents.

⊙ Key elements → Roles (eg → incident co-ordinator), timelines (eg → escalation within 1 hr) and communication protocols.

④ Remote Work Policy :-

→ Secure off-site work by addressing

⊙ Key elements :- Mandatory VPN use, MFA, and endpoint protection (antivirus).

⑤ Data Classification Policy :

→ Categorize data based on sensitivity (eg - public, confidential).

→ Key elements : Labeling requirements, access control and handling instructions.

⊙ Core Components of Security Procedure

⊙ Phishing Response Procedure :-

- Steps : Isolate affected device, notify SOC (Security Operations Center), document incident details (eg email sender, time), escalate to Tier 2 if needed, and follow-up with user training.

⊙ Password Managment Procedure

No.
Date

:-> Same generate strong password, update every 90 days.

⊙ Incident Reporting Procedure :

• Steps : Detect anomaly (eg) via SIEM alert), log incident in a tracking system, assign to response team, contain threat, and document resolution.

⊙ Remote Access Procedure :

• Steps : Connect via VPN, enable MFA, scan device for malware, log access and disconnect after use.

⊙ Data - Handling Procedure :

• Steps : Classify data (eg) confidential), encrypt sensitive files, restrict access to authorized personnel, and archive or destroy per retention policy.

No.
Date

Section-4 : Development and Implementation

• Steps to create :-

a) Needs Assessment : Identify assets (eg → servers, customer data) & risks (eg → phishing).

b) Drafting : Involve stake-holders (eg IT, legal) to align with business goals and compliance

c) Review and Approval : Obtain sign-off from management (eg CISO) and legal teams.

d) Distribution :- Share with employee via training or as internet.

e) Enforcement : Monitor Adherence with audits and tools (eg) AD for password policy).

Tips

• Keep language clear & concise.

:) Update annually.

:) Include exception with approval process.

5) Importance & Benefits :-

• Importance :-

① Provides legal protection by demonstrating due diligence.
② Reduces human error through clear guidelines.
③ Ensures consistency across departments.

• Benefits :-

① Minimizes security breaches
② Supports compliance with laws.
③ Enhances organizational trust and reputation.

6) Challenges and Solutions :-

▲ Challenges :-

• Resistance : Employees may find policies restrictive (eg→ frequent password changes).
• Complexity : Detailed procedures can be hard to follow without training
• Outdated Policies : Lack of updates leaves gaps (eg→ Missing MFA

▲ Solutions :-

• Conduct regular awareness training build acceptance.
• Use flowcharts or templates to simp procedures
• Schedule annual review with inpu from security teams.

Section : Practical Applications and Key Activities :-

• Scenarios :
• Small Business : Implement a basic AUP and password procedure to secure remote workers.
• Enterprise :- Develop an IR policy for a multi-national with SOC integration.
• Key Activities :-
→ Draft a 200-word Acceptable Use

No.

Date

Policy for a tech firm.

- Create a step-by-step procedure for reporting a suspected phishing email.
- Design a checklist to audit compliance with the password policy.

(8-5/10)

No.

Date

MITRE ATT&CK, TTPs, and IOCs :-

Section 1 :- Introduction to MITRE ATT&CK

- **Definition :-** MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible, community-driven knowledge base that catalogs adversary behaviours based on real-world observations. Developed by MITRE Corporation in 2013 and released Publicly in 2015, it models the tactics, techniques, and procedures (TTPs) used by cybercriminals across the attack Life cycle.

- **Purpose :** Helps cybersecurity professional detect, prevent and respond to threats by providing a common language and framework for understanding adversary actions, especially post compromise.

- **Matrices :** Covers Enterprise (Windows, macOS, Linux, cloud), Mobile (ios), and ICS (Industrial Control Systems) environments with updates reflecting evolving threats.

Section 2 : MITRE ATT&CK Framework :-

▶ Structure :→

⊙ Tactics → Represent the 'why' or adversary goals (eg→ Initial Access, Persistence, Execution). There are 14 tactics in the Enterprise matrix, including Reconnaissance, Resource Development, and Impact.

⊙ Techniques :- Describe the 'how' or methods to achieve tactical goals (eg→ Phishing for Initial Access). Includes 188 techniques and 379 sub-technique (as of recent updates).

⊙ Sub-Techniques :- Granular actions with in techniques (eg→ Spear phishing Attachment under Phishing).

⊙ Procedures :- Specific implementations of techniques (eg→ using Powershell to inject malware).

▲ Key Features :-

PTO.

- Behavioral focus :- Tracks what attackers do, not just indicators, making it resilient to tool changes.
- Community-driven :- Contributions from 226+ countries to enhance accuracy.

Used in Threat Hunting, red teaming, gap analysis, SOC maturity assessments

▶ Section 3 :- TTPs (Tactics, Techniques, and Procedures).

1.) Tactics :-

:- The adversary's tactical objectives or reasons for actions (eg→ Credential Access to steal login details).

Eg) Reconnaissance (gather info), Initial Access (enter network), Execution (run malicious code), Persistance (maintain access), Privilege Escalation (gain higher access), Defense Evasion (avoid detection), Credential Access, Discovery (map network), lateral movement (spread internally), Collection (gather data), Command and Control (Communicate with system), Exfiltration (Steal data)

, Impact (disrupt operations).

- Insight → Tactics are unordered, not all occur in every attack, reflecting adaptive adversary strategies.

▸ Techniques

Specific methods to achieve a tactic.
(eg→ Brute force for Credential Access)

- Examples → Drive-by-Compromise (initial access), fileless storage (Defense Evasion), OS Credential Dumping (Credential Access).

▸ Sub-techniques :, Refine techniques
(eg→ Password Spraying under Brute force).

⊙ Insight → Techniques are platform-specific (eg→ Windows, Linux) and include detection opportunities (eg→ log monitor).

⊙ Procedures :-

→ Step-by-step actions adversaries take (eg→ using hashcat to crack password)

→ Eg→ APT29 using Spearphishing Attachment, injecting malware via Powershell.

⊙ Insight :- Procedures combine multiple techniques / sub-techniques, offering detailed attack signatures for defenders.

- Application → TTPs enable proactive defense by simulating attacks (red teaming) and tuning detection tools (eg SIEM rule)

▸ Section 4 : Indicators of Compromise (IOCs).

→ Observable artifacts or evidences that a system has been breached, used to detect and respond to attacks

⊙ Types :- ① Atomic, ② Computed, ③ Network, ④ HOST ⑤ Behavioral.

① Atomic IOCs :- Single data points (eg→ IP address 192.168.1.1, file hash MD5 : d41d8cd98f).

② Computed IOCs :- Complex patterns (eg→ unusual traffic spikes, registry changes).

③ Network IOCs :- Anomalous traffic (eg→ outbound SMTP to unknown domains).

④ Host IOCs :- System changes (eg→ new processes, modified files).

⑤ Behavioral IOCs :- User actions (eg- rapid failed logins).

▸ Pyramid of Pain (Classification) :-

- Hash Values :- Easily changed by attackers, low pain.
- IP/Domain :- Moderately changeable, medium pain.
- Tools : Harder to alter, higher pain.
- TTPs :- Most resilient, highest pain for attackers to change.

▸ Detection :→ Leveraged by SIEMs, EDRs & threat intelligence platforms. to trigger alerts, requiring validation to reduce false positives.

- Example :- Unknown executable in /tmp, sudden DNS queries to a malicious domain.
- Insight : IOCs are reactive; combining them with TTPs (behavioral focus) enchances proactive defense.

▸ Section 5 : Practical Applications and key activities.

- Uses → ① Threat Hunting : Search for TTPS/IOCs missed by automated system.
- Red Teaming : Simulate attacks using ATT&CK techniques.
- Gap Analysis : Access detection coverage against tactics.

⑥ Key activities :-

→ Map phishing attack to MITRE tactics (eg, Initial Access → Phishing → Spearphishing Attachment).

- List 5 IOCs for a ransomware incident (eg → encrypted files, new registry keys).
- Simulate a Brute Force technique and suggest a mitigation (eg → Account lockout).

▶ Attack Life Cycle

→ The sequence of stages an adversary follows, from planning to impact. While MITRE ATT&CK focuses on post-compromise, understanding the full lifecycle is key.

▶ Stages :- ① Reconnaissance
↓ ② Weaponization → Creating malicious payload.
↓ ③ Delivery
↓ ④ Exploitation
↓ ⑤ Installation → Deploying malware
↓ ⑥ Command & Control (C2)
⑦ Achieving Objective

▶ Relevance → Complements ATT&CK by covering pre-compromise phases, enabling pro-active defense (eg → blocking reconnaissance traffic).

▶ Intermediate Insight :- The lifecycle aligns with frameworks like the cyber Kill Chain, where each phase offers detection points (eg → monitor email gateways for delivery).

- Defense Models :-

→ Cyber Kill Chain : A lockhead Martin model with 7 phases (Reconnaissance to Action on Objectives), linear and focused on breaking the chain.

→ Diamond Model :- Analyze attack

No.

Date

relationships (adversary, capability, infra, victim), emphasizing pattern detection.

- These models enhance ATT&CK by providing alternative perspective - Kill chain for prevention, Diamond for correlation.

Defense Models:-

- ~~Cyber kill chain~~
- SIEM
- EDR
- IPS/IDS

→ Need ~~Depth~~ for juniors lvl roles (6.5/10).