IAM vs RBAC — Clear, Practical Explanation

Identity and Access Management (IAM)
IAM is a framework that defines **who** can access a system and **what** they can do. It manages identities (users, services, machines), authentication, authorization, and auditing. IAM is commonly used in cloud platforms like AWS, Azure, and GCP.

Key IAM Concepts:

- Users, roles, groups
- Policies and permissions
- Authentication methods (passwords, MFA, keys)
- Temporary vs permanent credentials
- Logging and monitoring (CloudTrail, audit logs)

Role-Based Access Control (RBAC)
RBAC is an **authorization model** where permissions are assigned to roles, and users are assigned to those roles. Users do not receive permissions directly. RBAC simplifies access management and reduces excessive privileges.

Key RBAC Concepts:

- Roles represent job functions
- Permissions are attached to roles
- Users inherit permissions via roles
- Easier access reviews and audits

IAM vs RBAC — Core Difference
IAM is the **entire identity and access system**. RBAC is **one authorization strategy** implemented inside IAM. Think of IAM as the engine, and RBAC as one of the driving rules.

Why SOC & Cloud Teams Care

- Over-permissioned IAM leads to account compromise
- Lack of RBAC increases blast radius during breaches
- Misconfigured IAM is a top cause in cloud security incidents
- RBAC + least privilege reduces attack surface

Best Practices

- Use roles instead of long-term users
- Apply least privilege strictly
- Enforce MFA everywhere
- Monitor IAM changes continuously
- Review access periodically