AWS IAM Security – Deep Dive (Advanced)

A comprehensive guide for SOC Analysts and Cloud Security Engineers covering AWS IAM from fundamentals to advanced real-world security practices.

1. What AWS IAM Really Is

AWS Identity and Access Management (IAM) is the centralized security service that controls authentication and authorization across AWS services. IAM is global and applies to all regions.

2. IAM Core Components

- IAM Users – Permanent human or service identities.
- IAM Roles – Temporary identities assumed by services or users.
- Policies – JSON documents defining permissions.
- Trust Policies – Control who can assume roles.
- Permission Policies – Control what actions are allowed.

3. IAM Users vs IAM Roles

IAM users use long-term credentials and are higher risk. IAM roles use temporary credentials and are the recommended approach for AWS services and cross-account access.

4. IAM Policies – Deep Understanding

Policies define permissions using Effect, Action, Resource, and Condition. Explicit deny always overrides allow.

5. Types of IAM Policies

- Identity-based policies.
- Resource-based policies.
- Permission boundaries.
- Service Control Policies (SCPs).

6. Principle of Least Privilege

Least privilege limits permissions to reduce attack surface and blast radius.

7. IAM Policy Evaluation Logic

- Explicit Deny → Deny

- Allow → Allow
- No match → Implicit Deny

8. IAM Security Best Practices

- Enable MFA for privileged accounts.
- Avoid root account usage.
- Use IAM roles instead of access keys.
- Enable CloudTrail.

9. IAM Attack Techniques

- Privilege escalation.
- Access key leakage.
- Over-permissive roles.
- AssumeRole abuse.

10. SOC Analyst Monitoring Focus

SOC analysts should monitor IAM role assumptions, policy changes, root account usage, and anomalous API activity.