SOC Study Notes – Incident Lifecycle & AWS IAM

Clear, simple notes written for SOC analysts and cloud security roles.

1. Incident Lifecycle Steps (SOC View)

- **Preparation:** Setting up tools, processes, logging, and training before incidents occur.
- **Detection & Identification:** Alerts are analyzed to confirm whether an incident is real.
- **Containment:** Limiting the spread by isolating systems or disabling access.
- **Eradication:** Removing malware, closing vulnerabilities, and eliminating attacker access.
- **Recovery:** Restoring systems and monitoring for reoccurrence.
- **Lessons Learned:** Reviewing the incident to improve security controls.

2. AWS IAM Concepts with Examples

- **AWS IAM:** Controls who can access AWS resources and what actions they can perform.
- **IAM User:** Permanent identity for humans. Example: Admin logging into AWS console.
- **IAM Role:** Temporary identity assumed by services. Example: EC2 accessing S3 using a role.
- **IAM Policy:** JSON document defining permissions. Example: Allow s3:GetObject on one bucket.
- **Least Privilege:** Grant only required permissions to reduce risk.