SOC Roles and Responsibilities

1. Tier 1 SOC Analyst (Alert Analyst)

Primary Responsibilities:

- Monitor security alerts and dashboards continuously.
- Perform initial triage to identify false positives.
- Escalate validated incidents to Tier 2 analysts.
- Document incidents and maintain logs.

2. Tier 2 SOC Analyst (Incident Responder)

Primary Responsibilities:

- Conduct in-depth investigation of escalated incidents.
- Correlate multiple data sources such as network traffic and endpoint logs.
- Determine impact and scope of incidents.
- Work with IT and IR teams for containment and remediation.

3. SOC Manager (Operations Lead)

Primary Responsibilities:

- Supervise day-to-day operations of the SOC team.
- Manage personnel, schedules, and training.
- Ensure incident handling and response meet SLA and quality standards.
- Communicate incident status with leadership and compliance officers.