🔹 **SOC Roles & Responsibilities (RACI)**

- **Threat Detection & Triage** → SOC Tier 1 (SIEM Alerts, IDS/IPS, Endpoint Logs)
- **Incident Escalation & Analysis** → SOC Tier 2 (Deep Investigation, Malware Analysis)
- **Remediation & Containment** → SOC Tier 3 (Threat Hunting, Patch Deployment)
- **Reporting & Documentation** → Incident Manager (RCA, Compliance, SLA Reports)
- **Post-Incident Review & Improvement** → SOC Leadership (Lessons Learned, KPI Review)

🔹 **Key Performance Indicators (KPIs)**

- **MTTD (Mean Time to Detect)** at the Threat Detection phase.
- **MTTR (Mean Time to Respond)** at the Incident Escalation phase.
- **Containment Time** at the Remediation phase.
- **Incident Closure Rate** at the Reporting phase.
- **Process Optimization Metrics** at the Post-Incident Review phase.