SOC COMPONENT

1. People (SOC Team Members):-

The human backbone of a SOC:

- **SOC Analysts (L1, L2, L3)** → Detect, investigate, and respond to threats.
- **Incident Responders** → Contain and remediate attacks.
- **Threat Hunters** → Proactively search for hidden threats.
- **SOC Manager** → Oversees operations and team performance.
- **Compliance & Risk Officers** → Ensure legal/regulatory requirements.

---

2. Process (SOC Workflows & Procedures):-

Standardized methods to ensure consistent security monitoring:

- **Incident Detection & Response (IDR)**
- **Triage & Escalation** (deciding priority of alerts)
- **Playbooks & Runbooks** (step-by-step procedures)
- **Change Management & Patch Management**
- **Reporting & Documentation**
- **Continuous Improvement (Lessons Learned)**

---

3. Technology Stack (Tools & Platforms):-

The tech foundation that powers the SOC:

- **SIEM (Security Information & Event Management)** – Collects and correlates logs.
- **SOAR (Security Orchestration, Automation & Response)** – Automates responses.
- **EDR/XDR (Endpoint/Extended Detection & Response)** – Endpoint threat visibility.

- **IDS/IPS (Intrusion Detection/Prevention Systems)** – Detects network intrusions.
- **Firewalls & WAF (Web Application Firewall)**
- **Threat Intelligence Platforms**
- **Vulnerability Scanners**

---

4. SOC Governance:-

Defines how the SOC operates and aligns with business needs:

- **Policies & Procedures** → Security rules and guidelines.
- **Compliance & Regulations** → GDPR, HIPAA, PCI-DSS, ISO 27001.
- **KPIs & Metrics** → MTTR (Mean Time to Respond), alert handling, SLA tracking.
- **Risk Management** → Assessing and reducing cyber risks.
- **Audits & Reviews** → Regular checks for improvements.

---

5. Data Sources:-

Logs and events that feed the SOC for monitoring:

- **Network logs** → Routers, firewalls, IDS/IPS.
- **Endpoint logs** → Servers, desktops, laptops.
- **Application logs** → Web apps, databases.
- **Cloud logs** → AWS, Azure, GCP.
- **Identity logs** → Active Directory, IAM systems.
- **Threat intelligence feeds**.

---

6. Threat Intelligence:-

Knowledge that helps predict, detect, and respond to cyber threats:

- **Indicators of Compromise (IoCs)** → Malicious IPs, hashes, domains.
- **Indicators of Attack (IoAs)** → Tactics, techniques, and procedures (TTPs).
- **Threat Feeds** → External sources (OSINT, commercial feeds).

- **Dark Web Monitoring** → Tracking leaked data or chatter.
- **Threat Actor Profiling** → Understanding attacker groups and motives.

✅ In short:-

- **People** → Who runs the SOC
- **Process** → How they work
- **Technology** → Tools they use
- **Governance** → Rules & alignment with business
- **Data Sources** → Where info comes from
- **Threat Intelligence** → Extra knowledge for proactive defense