CORE FUNCTIONS OF SECURITY OPERATION CENTER

1. Log Collection :

Log collection is the foundation of SOC operations. It involves gathering log data from:

- **Devices** (firewalls, routers, IDS/IPS)
- **Servers** (web, file, database)
- **Endpoints** (workstations, laptops)
- **Applications** (cloud services, internal apps)

Logs contain critical events like login attempts, file access, system changes, or communication activity. This data is continuously collected using agents or centralized log collectors. **Without logs, threat detection is nearly impossible**.

---

2. Reporting

The reporting function translates raw data and analysis results into understandable formats such as:

- **Dashboards**
- **Weekly/monthly security reports**
- **Compliance audit logs**
- **Incident reports**

These reports are used by:

- **Management** to understand the organization's risk posture.
- **Security teams** to improve performance.
- **Auditors/regulators** to ensure compliance with frameworks (e.g., ISO 27001, GDPR, HIPAA).

---

3. Research & Development

R&D in a SOC context refers to:

- Studying **new attack vectors** (e.g., zero-day vulnerabilities).
- Developing **custom detection rules** for tools like SIEM.
- Creating **automation scripts** for faster incident response.
- Testing **new security technologies** in lab environments.

This helps the SOC evolve and defend against **ever-changing threats**, rather than relying solely on existing tools.

---

4. Threat Intelligence

Threat intelligence provides contextual data about:

- **Indicators of compromise (IOCs)** like malicious IPs, domains, file hashes.
- **Tactics, Techniques, and Procedures (TTPs)** used by threat actors (from MITRE ATT&CK framework).
- **Threat feeds** (commercial, open-source, or government-based).

The intelligence helps the SOC detect known threats faster, and even **predict and prevent future attacks**.

5. Knowledge Base

A knowledge base stores:

- **Historical incident details** and their resolutions.
- **Playbooks**: documented procedures for responding to certain threat types (e.g., phishing, ransomware).
- **Checklists and guides** for analysts and responders.

This ensures consistency in operations, facilitates training, and helps onboard new team members.

---

6. Ticketing

Ticketing systems like **JIRA, ServiceNow, or RTIR**:

- Create tickets automatically when alerts are generated.
- Assign them to analysts with priority levels.
- Track all actions taken during investigation.
- Allow collaboration across teams.
- Maintain an **audit trail** for review and compliance.

This ensures **structured and traceable incident response**.

---

7. SIEM (Security Information and Event Management)

A SIEM is a core SOC technology that:

- **Ingests log data** from various sources.
- **Normalizes and correlates** the data for patterns or anomalies.
- **Generates alerts** for suspicious activity based on pre-defined rules, behavior analytics, or machine learning.

Popular SIEM tools: **Splunk, IBM QRadar, Microsoft Sentinel, ArcSight**.

SIEM enables **real-time threat detection** and centralized visibility

---

8. Aggregation & Correlation

Aggregation gathers data from multiple systems. Correlation finds relationships between different events. For example:

- A login from India at 2 AM followed by data exfiltration might trigger an alert.
- Multiple failed logins from one IP across several systems could indicate a brute-force attack.
- **A user accessing sensitive financial records (Event A), followed by that same user attempting to transfer a large file to an external cloud storage service (Event B), especially if this occurs outside of normal business hours, could trigger a high-priority alert indicating potential data exfiltration or insider threat.**

• **Correlation rules reduce false positives** and reveal complex, multi-step attacks.