🛡️ Introduction to Security Operations (SecOps)

1. What is Security Operations?

Security Operations = The people, processes, and technology that monitor, detect, analyze, and respond to cyber threats in real-time.
👉 It's the "command center" of cybersecurity.

---

2. Security Operations Center (SOC)

- A dedicated team + infrastructure that:
    - Monitors logs, networks, endpoints, apps.
    - Detects suspicious activities.
    - Responds to incidents.
    - Improves security posture.

🔷 SOC Functions

1. Monitoring & Detection → SIEM tools (Splunk, QRadar, ELK).
2. Incident Response (IR) → Handling breaches quickly.
3. Threat Hunting → Proactively finding hidden threats.
4. Digital Forensics → Investigating attacks, collecting evidence.
5. Vulnerability Management → Patching, scanning, reducing risks.

---

3. Security Operations Tools

- SIEM (Security Info & Event Management) – Splunk, QRadar, ArcSight.
- SOAR (Security Orchestration Automation Response) – Cortex XSOAR, Demisto.
- EDR/XDR – CrowdStrike, SentinelOne.
- IDS/IPS – Snort, Suricata.
- Threat Intelligence Platforms – MISP, ThreatConnect.

🎯 Careers in Security Operations

1. Career Path in SecOps

- Tier 1 Analyst (SOC Analyst – L1) → Monitor, triage alerts.
- Tier 2 Analyst (L2) → Deep analysis, handle incidents.
- Tier 3 Analyst / Threat Hunter → Advanced investigation, malware analysis.
- Incident Responder → Respond & contain breaches.
- SOC Manager → Manage SOC operations, strategy.
- Blue Team Engineer → Defense architecture.
- Red Team Specialist → Offensive security (ethical hacking).
- Cybersecurity Consultant → Advises businesses.
- CISO (Chief Information Security Officer) → Executive leadership role.

---

2. Salary Range (India Example 🇮🇳)

- SOC Analyst (L1) → ₹4–6 LPA
- SOC Analyst (L2/L3) → ₹6–12 LPA
- Incident Responder / Threat Hunter → ₹8–15 LPA
- Security Consultant → ₹10–20 LPA
- CISO → ₹40+ LPA

(Global salaries are 2x–5x higher 💵)

🌍 Global Cybersecurity Certifications

🔷 Beginner Level

- CompTIA Security+ → Entry-level, covers basics.

- EC-Council CEH (Certified Ethical Hacker) → Offensive security skills.
- Cisco CCNA Security / CyberOps → Networking + security focus.

🔷 Intermediate Level

- CompTIA CySA+ → Cybersecurity Analyst, SOC-related.
- GIAC (GSEC, GCIA, GCIH) → Various specializations.
- OSCP (Offensive Security Certified Professional) → Penetration testing.

🔷 Advanced / Management

- CISSP (Certified Information Systems Security Professional) → Global standard for security leadership.
- CISM (Certified Information Security Manager) → Focus on management & governance.
- CISA (Certified Information Systems Auditor) → Audit & compliance.

🔷 Cloud Security

- CCSP (Certified Cloud Security Professional)
- AWS Security Specialty, Azure Security Engineer, Google Cloud Security