SOC L1 Training Curriculum

1. Introduction to SOC & Cybersecurity

- What is a Security Operations Center (SOC)?
- Roles of L1, L2, L3 Analysts
- Security concepts: CIA triad, defense in depth
- Security operations workflow (Detection → Analysis → Response → Recovery)

2. Networking Basics

- OSI model & TCP/IP model
- Common protocols (HTTP, HTTPS, DNS, FTP, SMTP, SSH, RDP)
- Ports & services (well-known ports like 80, 443, 3389)
- Network devices: routers, firewalls, IDS/IPS
- Packet analysis with **Wireshark**

3. Operating System Fundamentals

- **Windows basics** (Event Viewer, registry, processes, services, logs)
- **Linux basics** (file system, system logs, journalctl, networking commands)
- Common system logs to monitor for attacks

4. Security Tools & Technologies

- **SIEM tools** (Splunk, ELK, QRadar, ArcSight)

- Firewalls (basic rules, monitoring)
- Antivirus & Endpoint Detection (EDR basics)
- IDS/IPS systems

5. Log Analysis & Monitoring

- What logs to collect: system, application, network, authentication
- Detecting suspicious activity (failed logins, privilege escalation, port scans)
- Correlating alerts in SIEM
- Creating simple SIEM queries

6. Incident Detection & Triage

- Understanding alerts (false positives vs true positives)
- Initial investigation steps
- Documenting incidents (ticketing systems like ServiceNow/JIRA)
- Escalation rules (when to pass case to L2)

7. Threat Intelligence Basics

- What is threat intelligence?
- IoCs (Indicators of Compromise): IPs, hashes, domains
- Using free intel sources (VirusTotal, AlienVault OTX, AbuseIPDB)

8. Case Studies & Attack Scenarios

- Detecting brute force attacks
- Spotting phishing attempts
- Malware-infected endpoint case
- DDoS alert analysis
- Insider threat indicators

9. Soft Skills for SOC Analysts

- Writing clear incident reports
- Communication with IT teams & management
- Working in shifts (24/7 SOC)
- Stress management

Hands-On Labs for SOC L1

- Set up a **SIEM (Splunk/ELK)** and ingest logs
- Detect failed login attempts (brute force detection)
- Analyze suspicious network traffic with Wireshark
- Use VirusTotal & OTX to investigate IoCs
- Create a simple SOC playbook (step-by-step triage guide)

SOC L1 Job Readiness

- Job role: **SOC Analyst / Security Analyst – L1**

- Salary in India: **₹3.5 – 6 LPA**
- Certifications that help:
    - **CompTIA Security+**
    - **EC-Council CSA (Certified SOC Analyst)**
    - **Splunk Core Certified User**
    - **Microsoft SC-200 (Security Operations Analyst)**