SOC L2 Training Curriculum

1. Advanced Log & Event Analysis

- Deep dive into SIEM queries (Splunk SPL, ELK queries, QRadar AQL)
- Correlation rules & use case creation
- Detecting **lateral movement, privilege escalation, persistence**
- Log sources: Active Directory, firewalls, EDR, cloud logs

2. Threat Hunting

- Proactive vs reactive threat hunting
- MITRE ATT&CK framework mapping
- Hunting with indicators: IPs, hashes, domains, registry changes
- Hunting without indicators: anomaly detection, baselining
- Tools: **Sigma, YARA, Zeek, Sysmon**

3. Malware & Endpoint Analysis (Basic)

- Malware types & attack lifecycle
- Static analysis (hashing, strings, VirusTotal)
- Dynamic analysis (sandboxing with Any.Run, Cuckoo)
- Memory forensics (Volatility basics)
- Investigating infected endpoints via **EDR**

4. Network Forensics

- PCAP analysis in **Wireshark & Zeek**
- Detecting data exfiltration attempts
- DNS tunneling & C2 (Command & Control) patterns
- Detecting DDoS and botnet traffic

5. Incident Response & Playbooks

- Incident lifecycle: Preparation → Detection → Containment → Eradication → Recovery
- Writing & following IR playbooks
- Hands-on with SOAR (Cortex XSOAR, Phantom)
- Escalation to L3 or IR team

6. Threat Intelligence Integration

- Consuming threat feeds (MISP, AlienVault OTX, AbuseIPDB)
- Automating threat intel enrichment in SIEM/SOAR
- Creating intel reports for SOC team

7. Cloud Security Monitoring

- Security logging in **AWS CloudTrail, Azure Sentinel, GCP Security Command Center**
- Detecting cloud misconfigurations
- Investigating cloud identity compromise

8. Case Studies & Hands-On Labs

- Investigate a phishing email → analyze header, link, attachment
- Hunt for a compromised user account (MFA bypass attempt)
- Detect lateral movement via **Pass-the-Hash** in Active Directory logs
- Incident response drill: ransomware outbreak simulation
- Write a Sigma rule to detect malicious PowerShell

SOC L2 Hands-On Tools

- **SIEM:** Splunk, ELK, QRadar
- **Threat Hunting:** Sysmon, Sigma, YARA, Zeek
- **Forensics:** Volatility, Autopsy, FTK Imager
- **Malware Analysis:** Cuckoo Sandbox, Any.Run
- **Threat Intel:** MISP, VirusTotal, OTX
- **SOAR:** Phantom, XSOAR

SOC L2 Job Readiness

- Job role: **SOC Analyst – L2 / Threat Hunter / IR Specialist**
- Salary in India: **₹6 – 12 LPA**
- Certifications that help:
    - **GCIA (GIAC Certified Intrusion Analyst)**
    - **GCFA (GIAC Forensic Analyst)**
    - **CHFI (Computer Hacking Forensic Investigator)**
    - **Splunk Power User / Admin**

- **Microsoft SC-200**