Session 1- Introduction to SOC Analyst Role & Career Path

1. What is a SOC?

SOC stands for Security Operations Center.
It is the command center of cybersecurity.
A team of analysts and engineers work 24/7 to monitor, detect, and respond to security incidents.
Functions like an airport control tower but for digital threats.

2. SOC Analyst Role

SOC Analysts are frontline defenders.
They watch real-time alerts, investigate suspicious activities, and prevent cyber-attacks from spreading.

Daily duties:

- Monitor SIEM dashboards.
- Investigate alerts and differentiate between false positives and real attacks.
- Escalate incidents to higher levels if complex.
- Create incident reports.
- Suggest improvements to detection and response systems.

3. Levels of SOC Analyst Career

L1 (Entry-Level / Junior SOC Analyst):

- Monitor alerts in SIEM.
- Perform first triage (decide if harmless or suspicious).
- Escalate to L2 if necessary.

L2 (Mid-Level / Incident Responder):

- Deep investigation of suspicious events.
- Contain threats (block IPs, isolate endpoints).
- Perform threat hunting.

L3 (Senior Analyst / Threat Hunter):

- Advanced forensics and malware analysis.
- Write detection rules and tune SIEM.
- Lead incident response.

SOC Manager / Lead:

- Manage the team and report to CISOs.
- Focus on compliance, strategy, and KPIs.

4. Skills Required

Technical Skills:

- Networking (TCP/IP, firewalls, ports).
- Operating systems (Windows, Linux).
- SIEM tools (Splunk, QRadar, Sentinel).
- Threat intelligence basics.

Soft Skills:

- Analytical thinking.
- Communication (incident reporting).
- Decision-making under pressure.

5. Career Path / Growth

SOC Analyst (L1) → SOC Analyst (L2) → Senior SOC / Threat Hunter → Incident Responder → SOC Manager → Security Architect → CISO

6.Future branches:

- Threat Hunting
- Digital Forensics
- Red Team / Pentesting
- Cloud Security
- Governance, Risk and Compliance (GRC)

7.Summary:

- SOC is the heart of cyber defense.
- SOC Analyst is the frontline defender.
- Clear growth ladder from L1 to Manager to Leadership roles.