1. Incident Response Basics

Incident Response (IR) is the process of identifying, managing, and resolving cybersecurity incidents (like malware infections, data breaches, or unauthorized access).

Key Stages:

1. **Preparation** – Build playbooks, train staff, and set up tools.
2. **Identification** – Detect and confirm an incident.
3. **Containment** – Stop the spread (e.g., isolate infected systems).
4. **Eradication** – Remove the threat (e.g., delete malware).
5. **Recovery** – Restore systems and monitor for reinfection.
6. **Lessons Learned** – Review what happened and improve defenses.

Tools:

- Ticketing systems (Jira, ServiceNow)
- IR platforms (Cortex XSOAR, TheHive)

---

2. Log Analysis (Windows Event Logs, Sysmon, etc.)

Log analysis is the process of reviewing system and application logs to detect suspicious activity.

Common Sources:

- **Windows Event Logs** – Tracks system, security, and application events.
- **Sysmon (System Monitor)** – A Windows tool that logs detailed system activity like process creation, network connections, and file changes.

What to Look For:

- Unusual login times
- Failed login attempts
- Unexpected PowerShell or script executions
- New services or scheduled tasks

Tools:

- Event Viewer (Windows)
- Log aggregation tools (Graylog, ELK Stack)

---

3. SIEM Fundamentals (Splunk, Elastic, Sentinel)

SIEM (Security Information and Event Management) platforms collect, normalize, and analyze logs from across your environment to detect threats.

What SIEMs Do:

- Aggregate logs from multiple sources
- Correlate events to identify patterns
- Trigger alerts based on detection rules
- Provide dashboards and reports

Popular SIEMs:

- **Splunk** – Powerful, flexible, widely used in enterprise environments.
- **Elastic Security (ELK Stack)** – Open-source, customizable.
- **Microsoft Sentinel** – Cloud-native SIEM integrated with Azure.

Example Use:

Detecting a brute-force attack by correlating multiple failed login attempts across systems.