Response Models

Both models **provide structure and ensure a systematic approach, reducing oversights and enabling continuous improvement**.

SANS PICERL Model

- **Preparation**: Develop response playbooks, train teams, and establish clear protocols.
- **Identification**: Detect, validate, and assess incidents.
- **Containment**: Limit the attacker's access without causing further harm.
- **Eradication**: Remove the attacker from the environment.
- **Recovery**: Restore normal operations securely.
- **Lessons Learned**: Review the response, document findings, and adjust protocols.

Google's IMAG (Incident Management at Google)

- Focuses on: **Speed, scalability, and post-incident documentation**. IMAG emphasizes rapid response, clear communication, and **robust post-mortem analysis** to learn from every incident.