Incident Response Workflow

Incident Response Workflow (detailed)

1) Detect: SIEM/Wazuh generates alert

2) Triage: Tier 1 validates and enriches with TI

3) Contain: Isolate host, block IPs

4) Eradicate: Remove malware, patch systems

5) Recover: Restore from clean backups

6) Lessons Learned: RCA and update rules