SOC Incident Metrics Analysis – Data Stealer Malware

Scenario

Simulated endpoint compromise involving data-stealer malware communicating with a C2 server.

Project description

Investigated a simulated data-stealer malware incident and analyzed SOC performance metrics including MTTD, MTTA, and MTTR. Tracked incident timeline from initial compromise through detection, acknowledgment, escalation, and remediation. Identified detection and response gaps to evaluate SOC efficiency and incident handling workflow.

Key Actions Performed

- Analyzed alert timeline to calculate MTTD (12 min), MTTA (10 min), and MTTR (51 min)
- Assessed alert handling workflow from L1 triage to L2 remediation
- Correlated detection and response times to evaluate SOC operational effectiveness

Skills Demonstrated

- SOC incident lifecycle analysis
- Security metrics (MTTD, MTTA, MTTR)
- Alert triage and escalation workflows
- Incident response coordination

Tools / Environment

- TryHackMe SOC Analyst labs
- Simulated SIEM alerts
- Endpoint and network telemetry

Outcome / Impact

- Demonstrated ability to evaluate SOC detection and response efficiency using industry-standard metrics.