Endpoint Detection Lab (Sysmon + ELK)

Executive Summary

This project demonstrates endpoint-level detection engineering using Sysmon, Winlogbeat, and the Elastic Stack. The goal was to collect high-fidelity telemetry, identify malicious behavior, tune noise, and build dashboards for rapid triage.

Screenshot Placeholder

Architecture

Windows 10 endpoint with Sysmon, Winlogbeat forwarding logs to Elasticsearch, Kibana dashboards, and Kali attacker machine.

Screenshot Placeholder

Implementation

Installed Sysmon with SwiftOnSecurity config, forwarded logs, simulated attacks (PowerShell misuse, brute-force), built dashboards.

Screenshot Placeholder

Detection Engineering

Created & tuned detections for suspicious PowerShell, anomalous parent-child processes, brute-force attempts, and registry persistence.

Screenshot Placeholder

MITRE ATT&CK; Mapping

Mapped alerts to T1059, T1112, T1078, T1021.

Screenshot Placeholder

Outcome

Delivered a high-fidelity detection playbook and investigation report demonstrating triage workflow.

Screenshot Placeholder