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.

Architecture

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

Implementation

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

Detection Engineering

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

MITRE ATT&CK; Mapping

Mapped alerts to T1059, T1112, T1078, T1021.

Outcome

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