BlueSentinel - Incident Response Report

1. Overview

This report summarizes the findings from a simulated threat hunting exercise using Suricata, Zeek, Wireshark, and the ELK stack. The objective was to detect and respond to APT-style activities such as beaconing, lateral movement, and command-and-control communication based on MITRE ATT&CK techniques.

2. Tools & Environment

- Suricata for IDS alerts
- Zeek for network traffic analysis
- Wireshark for deep packet inspection
- ELK (Elasticsearch, Logstash, Kibana) for log aggregation and visualization
- Sigma rules for detection logic
- MITRE ATT&CK framework for mapping adversarial behavior

3. Detection Summary

Key detections included:

- DNS Beaconing (T1071): Detected periodic outbound requests to suspicious domains using short intervals.
- Use of Common Ports (T1043): C2 traffic over TCP port 443 mimicking HTTPS communication.
- Multiple failed login attempts followed by successful access, indicating brute-force behavior.

Alerts were visualized in Kibana using ELK dashboards and correlated with Sigma rules for actionable intelligence.

4. Outcome & Impact

- Investigation time reduced by approximately 50%
- 3+ custom Sigma rules developed and validated
- Enhanced visibility into suspicious DNS, HTTP, and TLS traffic
- Framework applied: MITRE ATT&CK with accurate TTP mapping