Security Metrics and Executive Reporting

Tool Used: Wazuh SIEM
Scope: SOC Metrics Evaluation (MTTD, MTTR, False Positive Rate, Dwell Time)

Executive Summary (≈150 words)

This report highlights the main performance metrics of the Security Operations Center (SOC) based on the evaluation of the security alerts received from the Wazuh platform. The details of the security situation were clearly obtained as the calculated Mean Time to Detect of the security incidents was close to two hours from the presumed start of the suspicious activities.

The Mean Time to Respond was determined to be four hours, as this is the timeline from the detection of the alert to the mitigation of the simulated incidents. Whilst acceptable in the lab environment, the response can be optimized through the automation of the incident response workflow.

Furthermore, an examination of the quality of alerts showed that a false positive rate of 15% occurred due to benign system and authentication-related events. Too many false positives could overwhelm analysts and prolong wait times for valid threats.

For better SOC effectiveness, recommendations include the need to fine-tune the rules for better detection, reducing the amount of noise in the alert, as well as the need to incorporate automated responses. This would further minimize the time taken for the SOC, the time taken as a result of the SOC, as well as the possibility

Metrics Methodology

- **MTTD:** Estimated using alert timestamps and contextual analysis of suspicious activity.
- **MTTR:** Simulated analyst response time due to absence of automated response.
- **False Positive Rate:** Calculated through manual analyst review of alerts.
- **Dwell Time:** Derived from estimated compromise and detection times

Conclusion

The SOC metrics demonstrate functional detection and response capabilities within the current lab environment. However, improvements in alert tuning, automation, and response orchestration are necessary to enhance operational efficiency and reduce security risk.