Security Metrics and Executive Reporting Report

1. Executive Summary

This report documents the measurement, analysis, and executive reporting of key Security Operations Center (SOC) performance metrics using Elastic Security, Google Sheets, and Google Docs. The objective is to assess detection efficiency, response effectiveness, and overall SOC maturity using industry-standard metrics such as MTTD, MTTR, False Positive Rate, and Dwell Time.

2. SOC Metrics Dashboard Implementation

2.1. Mean Time to Detect (MTTD)

MTTD measures the average time taken to detect a security incident from the moment malicious activity begins.

Formula:

MTTD = Detection Time – Attack Start Time

Observed Result:

- **MTTD: 2 Hours**

2.2. Mean Time to Respond (MTTR)

MTTR measures the time required to investigate, contain, and remediate an incident after detection.

Formula:

MTTR = Incident Closure Time – Detection Time

Observed Result:

- **MTTR: 4 Hours**

2.3. False Positive Rate

The percentage of alerts incorrectly classified as malicious.

Formula:

(False Positives ÷ Total Alerts) × 100

Observation:

False positive rates were within acceptable SOC thresholds, indicating well-tuned detection rules.

3. Dwell Time Analysis

Dwell time represents how long an attacker remains undetected within the environment.

Calculation Method:

- Attack Start Time (event.start)
- Containment Time (event.end)

Observed Dwell Time:

- **6 Hours**

Although detection was timely, earlier behavioral detection could further reduce exposure risk.

4. Executive Summary

During the reporting period, the SOC demonstrated strong detection and response performance. Mean Time to Detect (MTTD) averaged 2 hours, confirming effective monitoring and alerting mechanisms. Mean Time to Respond (MTTR) averaged 4 hours, reflecting efficient incident handling, containment, and remediation workflows. False positive rates remained controlled, indicating mature alert tuning and reduced analyst fatigue.

Dwell time analysis identified an average attacker presence of 6 hours, suggesting opportunities to enhance early-stage detection through advanced correlation rules and proactive threat hunting. Strategic recommendations include increased automation, expanded endpoint telemetry, and continued analyst training. Overall, SOC operations exhibit a mature security posture supported by measurable, actionable metrics aligned with industry best practices.