Title: Security Metrices and Executive Summary

Date: 24 Nov 2025
Prepared by: Mayuri Sawle

1. Metrics Dashboard (Elastic Security)

Key Metrics
MTTD (Mean Time to Detect):
Time from threat occurrence → first alert
Example: 2 hours

MTTR (Mean Time to Respond):
Time from first alert → containment
Example: 4 hours

False Positive Rate:
False Positives / Total Alerts × 100

2. Executive Summary

Executive Summary (150 words):

Over the past reporting period, the Security Operations Center (SOC) demonstrated improved responsiveness through measurable gains in detection and remediation times. The average Mean Time to Detect (MTTD) was two hours, reflecting timely alert visibility and effective use of Elastic Security's analytics. Mean Time to Respond (MTTR) averaged four hours, showing coordinated containment and incident-handling procedures across the SOC team. False positive reduction initiatives also showed progress, decreasing unnecessary analyst workload and improving overall operational efficiency. Continued focus on alert tuning, enhanced playbook automation, and expanded use of behavioral analytics will further strengthen detection accuracy. To advance performance, the SOC should invest in ongoing analyst training, automate repetitive triage tasks, and enhance correlation rules to reduce noise. These efforts will shorten investigation cycles, improve dwell-time reduction, and provide stronger protection against emerging threats while supporting strategic business continuity objectives.

3. Dwell Time Analysis (Google Sheets)

How to Calculate:
Dwell Time = Attack Start Time – Remediation Completion Time
Attack began: 08:00
Fully remediated: 14:00
Dwell Time = 6 hours

Summary (50 words):

The dwell-time analysis shows a six-hour gap between initial compromise and full remediation. This duration highlights effective detection and response processes but indicates room for improvement in early identification and automated containment. Reducing dwell time will directly limit attacker persistence and minimize operational and security risks.