Security Metrics and Executive Reporting

1 Metrics Dashboard (Elastic Security)

Metrics Calculated (Mock Incident Data)

Metric	Value	How It Was Calculated
MTTD (Mean Time to Detect)	**2 hours**	Detection Time – Attack Start Time
MTTR (Mean Time to Respond)	**4 hours**	Incident Closure Time – Detection Time
False Positive Rate	**20%**	(False Alerts / Total Alerts) × 100

Example Dataset (for Elastic / Sheets)

Incident ID	Attack Start	Detection Time	Response End	True/False
INC-01	10:00	12:00	16:00	True
INC-02	11:00	13:00	17:00	True
INC-03	12:00	12:30	—	False
INC-04	13:00	13:15	—	False
INC-05	14:00	14:30	18:30	True

False Positive Rate
= 2 False Alerts / 10 Total Alerts × 100
= **20%**

Elastic Security Dashboard Widgets

Create these visualizations:

- 📊 **Bar Chart** → MTTD per incident
- 📈 **Line Chart** → MTTR trend over time
- 🟡 **Pie Chart** → True vs False Alerts
- 🔢 **Metric Widget** → Average MTTD & MTTR

2️⃣ Executive Summary (150 words – Google Docs)

Executive Summary

During the analysis period, the Security Operations Center (SOC) demonstrated moderate detection and response efficiency. The Mean Time to Detect (MTTD) was measured at 2 hours, indicating that threats are identified within an acceptable timeframe but still leave room for faster alert triage. The Mean Time to Respond (MTTR) averaged 4 hours, reflecting effective containment and remediation processes once incidents were confirmed. However, the false positive rate of 20% highlights alert noise that impacts analyst productivity and response prioritization.

Dwell time analysis showed attackers remained active in the environment for an average of 6 hours before full containment, increasing potential risk exposure. To improve SOC performance, it is recommended to enhance alert tuning in Elastic Security, integrate threat intelligence feeds, and automate initial triage workflows. Continuous dashboard monitoring and regular executive reporting will support faster decision-making and strengthen the organization's overall security posture.

3 Metrics Analysis – Dwell Time

Dwell Time Calculation

Incident	Initial Compromise	Containment Time	Dwell Time
INC-01	10:00	16:00	6 hours
INC-02	11:00	17:00	6 hours
INC-05	14:00	18:30	4.5 hours

Average Dwell Time: ~5.5 hours

50-Word Dwell Time Summary

The average dwell time of approximately 5.5 hours indicates that attackers maintained access for a significant duration before containment. Reducing detection delays and improving automated response actions can significantly lower dwell time, minimizing attacker impact and reducing the overall risk to critical systems.