Security Metrics and Executive Reporting

Introduction

This document provides a detailed guide for calculating advanced security metrics and creating executive reports using mock incident data. It outlines the steps to create mock incidents, compute metrics such as Mean Time To Detect (MTTD), Mean Time To Respond (MTTR), and false positive rate, and generate dashboards and reports for SOC performance evaluation.

Creating a Mock Incident

Define the Scenario

- Choose a realistic attack type (e.g., phishing, ransomware, brute-force login).
- Assign an Incident ID (e.g., INC-001).
- Define severity and alert outcome (true_positive/false_positive).

Create Timeline Events

Stage	Timestamp	Notes
Initial Compromise	2025-09-01 09:15:00	First seen
Detection	2025-09-01 11:20:00	Alert triggered
Containment	2025-09-01 15:40:00	SOC response
Closure	2025-09-01 17:00:00	Incident resolved

Add Metadata

- **Rule Name:** Suspicious Link Click
- **Alert Outcome:** true_positive
- **Severity:** High

Insert Into Google Sheets

Incident ID	First Seen	Alert Created	Containment Time	Alert Outcome	Detection Latency (hrs)	Response Time (hrs)	Is False Positive
INC-001	2025-09-01 09:15:00	2025-09-01 11:20:00	2025-09-01 15:40:00	true_positive	=(C2-B2)*24	=(D2-C2)*24	=IF(E2="false_positive",1,0)

Metrics Dashboard Configuration (Elastic Security)

- MTTD: Avg detection latency (detection_time - initial_event_time)
- MTTR: Avg response time (containment_time - detection_time)
- False Positive Rate: (false_positive_count / total_alerts) * 100

Additional visualizations:

- Alerts volume over time by severity and rule
- Top noisy rules by false positives
- Dwell-time distribution (percentiles: P50, P90, P99)

Google Sheets Metrics Calculation

- Total alerts: =COUNTA(A2:A1000)
- MTTD: =AVERAGE(F2:F1000)
- MTTR: =AVERAGE(G2:G1000)
- False Positive Rate: =SUM(H2:H1000)/COUNTA(A2:A1000)*100
- Charts: bar chart for false positives, line chart for MTTD & MTTR

Executive Report

50-Word Summary

In the last quarter the Security Operations Center (SOC) measured key metrics to assess detection and response capability. Mean Time To Detect (MTTD) averaged 2 hours

and Mean Time To Respond (MTTR) averaged 4 hours. While these timings meet several operational goals, a high false positive rate of 18% is degrading analyst productivity and increasing time-to-containment. Dwell-time analysis of a representative phishing incident showed that attackers remained active for an extended period due to manual triage queues and inconsistent playbook use. To improve performance we recommend three priority actions: (1) tune and retire noisy signatures and refine correlation rules to reduce false positives, (2) implement automated containment playbooks for high-confidence alerts to shorten MTTR, and (3) invest in targeted analyst training and proactive threat hunting to lower dwell time. Implementing these measures should reduce alerts triage load, improve response consistency, and deliver measurable gains in detection and containment. and resilience.

50-Word Dwell-Time Summary

Dwell-time analysis of the mock phishing incident showed attackers persisted for 18 hours due to delayed triage and lack of automated containment. Manual workflows and alert fatigue extended exposure. Recommendation: automate containment for high-confidence alerts, streamline triage playbooks, and increase proactive hunting to reduce dwell time and exposure and remediation.

Recommended Workflow

- Create ingest pipeline fields: initial_event_timestamp, detection_time, containment_time, dwell_time_hours
- Build dashboard panels for MTTD, MTTR, False Positive Rate
- Identify and tune noisy rules
- Implement automated playbook for high-confidence detection
- Run one-week retrospective in Sheets and present executive summary

References

- Elastic Security Documentation: https://www.elastic.co/guide/en/security/current/index.html
- Phishing Simulation Example: https://www.csoonline.com/article/3534941/phishing-explained.html