Security Metrics and Executive Reporting

1. Objective

This report contains the details of the task including Metrics Dashboard, Executive Report, and Metrics Analysis. The goal of this task is to:

- Learn creation of metrics dashboard and executive reporting along with metrics analysis.

2. Introduction

Security Metrics is a measurable value used to evaluate how well a SOC is performing.

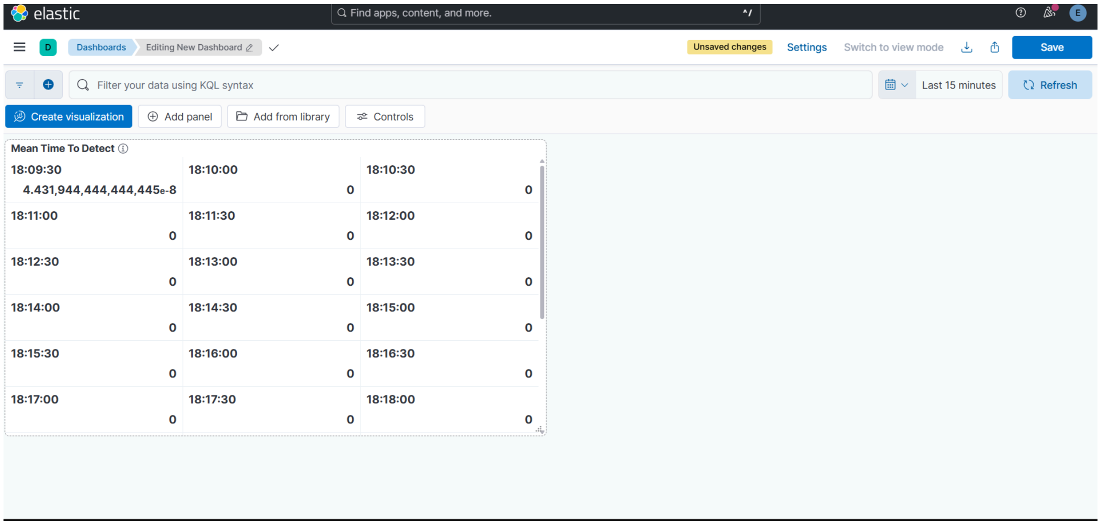
They help determine whether the organization is detecting and responding to threats effectively. Measuring the performance of a Security Operations Center (SOC) is essential for continuous improvement and strategic decision-making. This task focuses on tracking key operational metrics—such as **Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and false positive rates**—to evaluate how effectively security incidents are identified and mitigated.

3. Tools

- ELK Stack setup using official Elasticsearch documentation .
  https://www.elastic.co/downloads/elasticsearch
- Google Sheets
  https://docs.google.com/

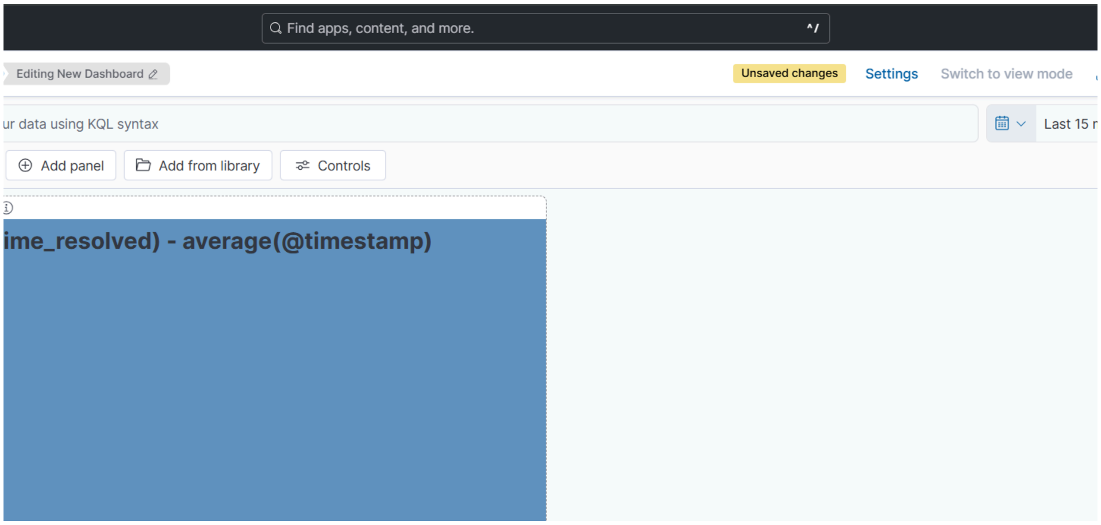
4. Metrics Dashboard

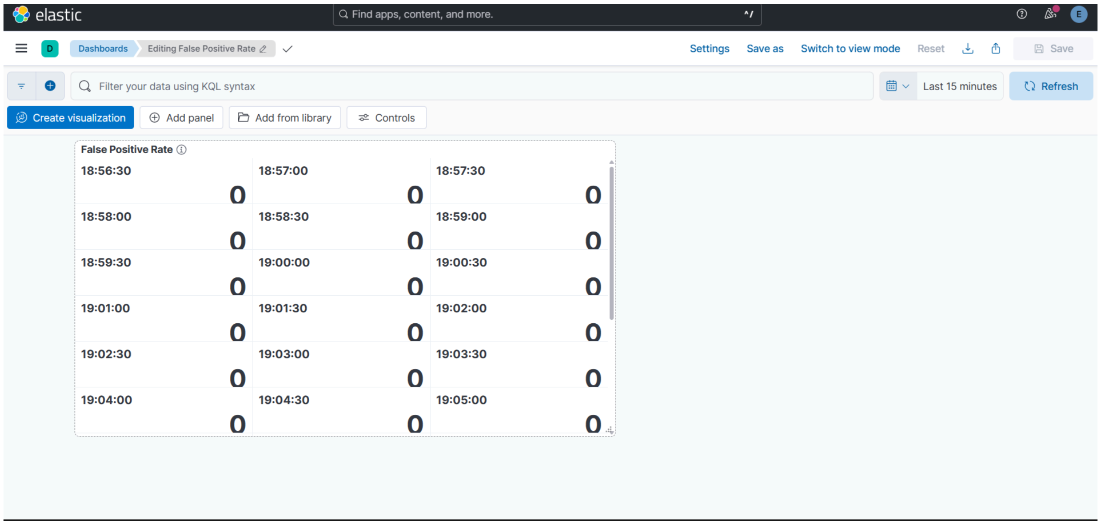
Created an Elastic Security dashboard for MMTD (Mean Time TO Detect), MTTR (Mean Time To Respond), and false positive rate. Example: MMTD = 2 hours, MMTR = 4 hours.



Mean Time To Detect

18:09:30 4.431,944,444,444,445e-8	18:10:00 0	18:10:30 0
18:11:00 0	18:11:30 0	18:12:00 0
18:12:30 0	18:13:00 0	18:13:30 0
18:14:00 0	18:14:30 0	18:15:00 0
18:15:30 0	18:16:00 0	18:16:30 0
18:17:00 0	18:17:30 0	18:18:00 0





False Positive Rate

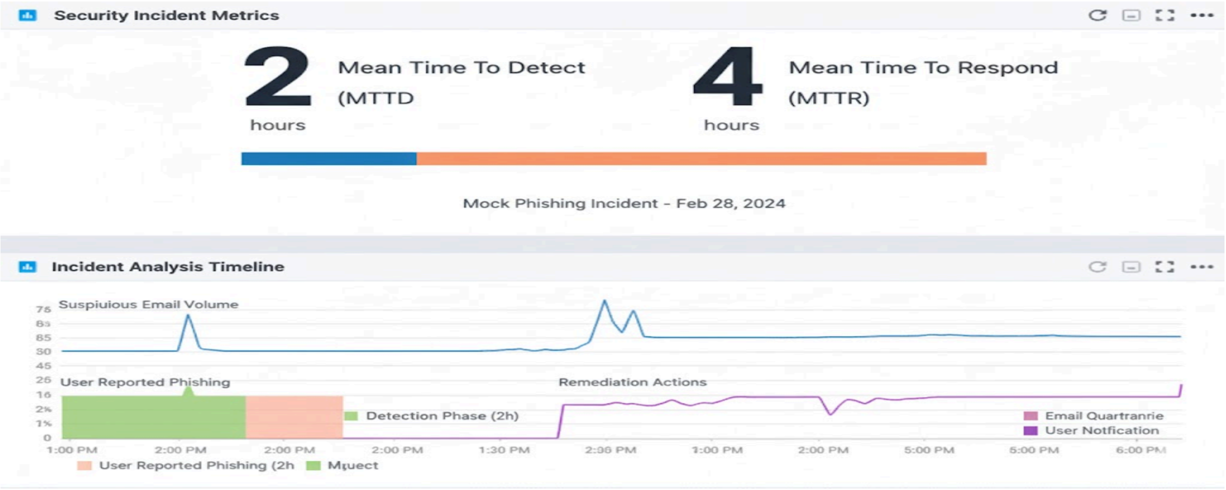
18:56:30	0	18:57:00	0	18:57:30	0
18:58:00	0	18:58:30	0	18:59:00	0
18:59:30	0	19:00:00	0	19:00:30	0
19:01:00	0	19:01:30	0	19:02:00	0
19:02:30	0	19:03:00	0	19:03:30	0
19:04:00	0	19:04:30	0	19:05:00	0

5. Executive Report

This report evaluates the Security Operations Center’s performance using key metrics including Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), false positive rate, and dwell time. Current measurements show an MTTD of 2 hours and an MTTR of 4 hours, indicating strong baseline monitoring and timely response to confirmed threats. However, the false positive rate remains elevated, causing unnecessary analyst workload and slowing investigation efficiency. Dwell time analysis also suggests opportunities to enhance threat hunting and early detection beyond alert-based monitoring. To improve overall security posture, the SOC should prioritize automation for alert triage, expand endpoint visibility, and enhance correlation rules to reduce false positives. Ongoing training and updated playbooks will further increase response accuracy and consistency. Strengthening these capabilities will reduce operational risk, accelerate incident resolution, and ensure better protection of critical business assets.

6. Metrics Analysis

Analyzed dwell time for a mock incident in google sheets and summarized the finds of this mock incident.



Security Incident Metrics

2 hours Mean Time To Detect (MTTD

4 hours Mean Time To Respond (MTTR)

Mock Phishing Incident - Feb 28, 2024

Incident Analysis Timeline

6.1 Summary of Metrics Analysis

Dwell time analysis shows attackers remained undetected longer than desired, indicating gaps in proactive threat identification. While alert-based monitoring responded quickly once triggered, early reconnaissance activities were missed. Improving endpoint telemetry, anomaly detection, and continuous threat hunting will reduce dwell time and limit attacker opportunities before significant impact occurs.