Security Metrics and Executive Reporting

Security metrics were analyzed to evaluate SOC performance and identify improvement opportunities. Key performance indicators (KPIs) including Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), False Positive Rate, and Dwell Time were reviewed using dashboard visualization and metric calculations.

Metrics Dashboard Overview

An Elastic Security dashboard was designed to monitor the following:

- **MTTD (Mean Time to Detect):** 2 Hours
- **MTTR (Mean Time to Respond):** 4 Hours
- **False Positive Rate:** 12%

The dashboard provided visual insight into detection efficiency, response effectiveness, and alert accuracy trends over time. These metrics help leadership understand SOC operational performance.

Dwell Time Analysis (50 Words)

The mock incident revealed a dwell time of approximately 2 hours between initial compromise and detection. While detection occurred relatively quickly, reducing dwell time further through enhanced monitoring and behavioral analytics would strengthen proactive defense and minimize potential impact from future threats.

Executive Summary

The Security Operations Center demonstrated effective monitoring and response capabilities during the evaluation period. The Mean Time to Detect (2 hours) and Mean Time to Respond (4 hours) reflect structured workflows and timely containment actions. However, a false positive rate of 12% indicates room for improvement in alert tuning and detection rule optimization. Reducing unnecessary alerts will allow analysts to focus on high-risk incidents and improve overall efficiency. Dwell time analysis highlights the importance of strengthening early detection mechanisms to limit attacker presence within the environment. Recommended improvements include enhanced behavioral analytics, periodic rule reviews, automated enrichment workflows,

and continued analyst training. Implementing these enhancements will further reduce response times, improve detection accuracy, and strengthen the organization’s overall security posture.