Executive Summary

The Security Operations Center's performance metrics indicate an average Mean Time to Detect (MTTD) of two hours and a Mean Time to Respond (MTTR) of four hours during the reporting period. The calculated dwell time for the analyzed incident was six hours, reflecting the total exposure window before containment. While detection capabilities demonstrate reasonable efficiency, response duration suggests opportunities for process optimization and automation.

The false positive rate remains within manageable limits; however, further tuning of correlation rules and threat intelligence enrichment could improve analyst productivity and reduce alert fatigue. To enhance SOC effectiveness, it is recommended to implement automated containment actions through SOAR integration, refine detection logic for high-confidence alerts, and conduct regular response simulations to reduce MTTR. Continuous metric tracking through Elastic dashboards will ensure measurable improvement and executive visibility.

Dwell Time Summary

Dwell time analysis revealed the attacker remained active for six hours before containment. Detection occurred within two hours, while response actions required four additional hours. Although detection performance is acceptable, reducing response time could significantly minimize operational risk and potential lateral movement exposure.