Executive Summary

Subject: Security Operations Center (SOC) Performance Summary and Recommendations

The security posture analysis reveals mixed performance, with a concerning gap in threat lifecycle management. Our Mean Time to Detect (MTTD) is 2 hours, which is acceptable, but the Mean Time to Respond (MTTR) is 4 hours, indicating slow containment and remediation. Critically, the False Positive Rate (FPR) of 5% is manageable, yet the high MTTR suggests analysts may be spending too much time on legitimate but non-critical alerts or lacking automated response playbooks.
A recent incident analysis highlighted a 30.5-hour dwell time, underscoring the need for faster, higher-fidelity detection.

Recommendations: We recommend an investment to enhance security orchestration, automation, and response (SOAR) capabilities to cut MTTR by 50% and reduce manual workload. Furthermore, a review of core log sources is needed to reduce detection latency and lower the maximum dwell time.