# Executive Summary

Analysis of 1,000 Wazuh security alerts from September 1-29, 2025 across three monitored agents (DESKTOP-IROTPGQ, kali, wazuh-server) revealed exceptional threat detection capabilities with critical remediation gaps. Mean Time To Detect (MTTD) of 121.49 seconds demonstrates world-class monitoring infrastructure. Zero false positives indicate mature rule tuning. However, dwell time analysis exposes significant concern: DESKTOP-IROTPGQ exhibited 33.37-hour threat persistence, followed by kali at 30.78 hours and wazuh-server at 27.99 hours. All agents exceed acceptable 24-hour threshold, indicating systematic response delays. Critical Action Required: Implement automated response playbooks to reduce dwell times and investigate DESKTOP-IROTPGQ's elevated persistence patterns.

## Dwell Time Summary

Dwell time measures threat persistence from detection to remediation. DESKTOP-IROTPGQ experienced longest exposure at 33.37 hours, exceeding wazuh-server baseline (27.99 hours) by 19.2%. Extended dwell times across all systems indicate systematic response delays requiring immediate automated containment deployment and enhanced incident workflow optimization.