Intelligent iT

The Difference Between Detecting a Threat and Stopping One

Why Detection Alone Isn't Protection

Detection without action is surveillance. Many organizations have sophisticated detection systems but fail to implement rapid response, leaving threats active for extended periods. The gap between detection and response is where breaches happen.

The Response Gap Problem

Alert generated 3 AM. Analyst reviews alert 8 AM. Investigation begins 8:15 AM. Containment starts 9 AM. By then: 6 hours have passed. With exfiltration occurring in 72 minutes, the attacker has already copied critical data. Detection succeeded. Response failed.

Automated Response Accelerates Protection

Manual response is slow. Automated investigation (collect logs, analyze behavior, determine scope) and containment (isolate systems, disable credentials) accelerate critical functions. Organizations with automated response show 3-5x faster containment. That speed differential determines whether threats are contained during reconnaissance or after critical damage.

Outcomes Over Alerts

Don't measure detection capability. Measure outcomes: Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), dwell time reduction, incident damage reduction. A sophisticated detection system that takes 200 days to find a breach and 4 hours to respond is less valuable than a simpler system that finds threats in 12 minutes and responds in 5.

Key Statistics

72 minutes: Time to exfiltration | 3-5x faster with automation | Industry average MTTD: 200+ days | Leading organizations: 12 minutes

Bridge the Gap

Unified Core automates investigation and response—threats are not just detected, they're contained. Automated baseline procedures free analysts to focus on decisions requiring judgment. In a threat landscape where exfiltration occurs in 72 minutes, response speed determines outcomes. Manual response is already too slow.