Intelligent IT

Run Books and Defined Response

Why Winging It During an Incident Costs You Everything

When threats are detected, every second matters. Organizations with documented response procedures—run books—respond 3-5 times faster than those making decisions in real-time. With intrusions reaching data exfiltration in 72 minutes, the difference between 5-minute and 45-minute response initiation determines whether attacks are contained during reconnaissance or after critical data is lost.

The Speed Difference

Without run books: Alert → Interpretation (5 min) → Manager notification (5 min) → Decision-making (10 min) → Approval (10 min) → Response begins (45 minutes after detection).

With run books: Alert → Procedure execution → Response begins (5 minutes after detection).

This 40-minute difference translates to vastly different outcomes—attacks contained during reconnaissance versus after critical data exfiltration.

Anatomy of Effective Run Books

Clear threat definitions → Immediate actions (isolate, preserve evidence, notify) → Investigation procedures (scope, impact, lateral movement) → Escalation criteria → Communication procedures → Return-to-service validation.

Most effective when specific to your environment, tested regularly, and continuously updated.

Building Your Playbook

1) Identify common threats. 2) Map current processes. 3) Eliminate decision delays. 4) Document step-by-step procedures. 5) Test through tabletop exercises. 6) Iterate based on experience.

Key Statistics

72 minutes: Time to data exfiltration | 3-5x faster response with documented procedures | 70% higher SOC turnover without automation

Documented Response Wins

Organizations with effective run books show consistently shorter dwell times, faster containment, and lower incident damage. Unified Core platform supports documented response through comprehensive logging, investigation capabilities, and playbook-driven automation—enabling rapid response without requiring every analyst know every procedure.