Intelligent iT

What Actually Happens During a Cyber Incident

A Step by Step Breakdown

Cyber incidents follow predictable phases. Understanding detection, containment, eradication, recovery, and review enables more systematic response. This condensed guide walks through each phase of a realistic incident.

Detection & Triage

An alert is generated. Triage determines if it's a real threat (not a false positive) and establishes scope and criticality. Context matters—same alert patterns mean different things in different scenarios.

Containment (The Emergency Stop)

Isolate systems, disable compromised accounts, block attacker C2 communications, prevent exfiltration, preserve evidence. Speed matters—containment during reconnaissance means minimal damage. Containment after exfiltration begins means significant damage.

Eradication (Complete Removal)

Root cause analysis. Remove persistence mechanisms. Clean lateral movement. Reset compromised credentials. Patch vulnerabilities. This is where organizations often fail—declaring incidents closed before persistence is fully removed. Incomplete eradication enables re-infection.

Recovery & Validation

Rebuild or restore systems. Validate data integrity. Test functionality. Gradual service restoration. Patient return to production prevents re-activating hidden backdoors.

Post-Incident Review

Timeline analysis. Detection quality assessment. Response quality evaluation. Root cause confirmation. Prevention planning. Organizations that systematically extract lessons improve their security posture over time.

Key Statistics

72 minutes: Detection to exfiltration | 22%: Credential abuse leading breach vector | 94 days: Average credential remediation

Moving Forward

Unified Core supports incident response at every phase—detection, containment, eradication, recovery, and review. By providing visibility and automation at each step, organizations move through response systematically rather than reactively.