
Smarttech
YOUR 24/7 SECURITY PARTNER
Full-Spectrum
INCIDENT RESPONSE

# One incident. One team. Every angle covered.

Most serious attacks don't stay in one lane. A phishing email leads to an account takeover, which drops malware, which abuses OAuth apps to exfiltrate data. If your response is siloed by tool or technology, you're always playing catch-up.

Our Full-Spectrum Incident Response service delivers a single, integrated response capability across identity, email, endpoint, and cloud – regardless of whether you use CrowdStrike, Microsoft, Cortex, Proofpoint, Abnormal, or a combination.

## THE CHALLENGES WE SOLVE

- Fragmented visibility across multiple vendors and consoles.
- Different teams owning different tools, with no one accountable for the overall incident.
- Repeated handoffs slowing down containment while attackers move on.
- Inconsistent documentation and lessons learned across incidents.

## WHAT YOU GET

- Unified incident command: one team owning the investigation across email, identity, endpoint, and cloud apps.
- Cross-tool correlation: we connect detections from CrowdStrike, Microsoft 365 Defender, Cortex, Proofpoint, Abnormal and others into one storyline.
- End-to-end attack path reconstruction: initial vector → privilege escalation → lateral movement → data access → exfiltration attempts.
- Coordinated containment: aligned actions on accounts, devices, mailboxes, and cloud resources based on a single, agreed playbook.
- Business-level incident reporting: non-technical summaries, impact assessments, and recommendations for executives and boards.
- Continuous improvement: playbook tuning, detection gap analysis, and technology alignment across your stack.

## HOW IT WORKS

1. Prepare: We onboard your tools, agree playbooks and escalation paths, and rehearse likely scenarios.
2. Detect & declare: When an incident hits, we declare a unified case and bring together signals from all relevant systems.
3. Investigate & contain: Our analysts work the case across domains, closing off attacker routes as we go.
4. Recover & improve: We guide clean-up, provide evidence for internal/external stakeholders, and feed findings back into controls.

## WHY ORGANISATIONS CHOOSE US

- Multi-vendor fluency: We speak Microsoft, CrowdStrike, Palo, Proofpoint, Abnormal and more – so you don't have to consolidate vendors to get integrated response.
- Operates like an in-house team: You know who's on your case, how to reach them, and how decisions are made.
- Outcome obsessed: Faster containment, reduced impact, and a clear pathway to improving your security posture, not just surviving the incident.

# Ready to get started?

Ask us how we'd handle your worst-case scenario

info@smarttech247.com