Smarttech
YOUR 24/7 SECURITY PARTNER

Identity Incident Response

Stop account takeovers before they become breaches

Attackers no longer need to “break in” when they can simply log in using stolen or abused credentials. Password spraying, MFA fatigue, token theft and session hijacking now sit at the centre of most major breaches.

Our Identity Incident Response service gives you a specialist team focused on one thing: detecting and containing identity compromise across Entra ID, CrowdStrike identity, and other IdPs before it spreads.

THE CHALLENGES WE SOLVE

- Users approve MFA prompts they shouldn’t – and no one notices until it’s too late.
- Risky sign-in and impossible-travel alerts pile up in consoles with no one truly owning them.
- OAuth apps, service principals, and non-human identities create blind spots attackers love.
- Security teams waste hours sorting false positives from genuine account takeovers.

WHAT YOU GET

- 24x7 monitoring of risky identity signals across supported platforms (e.g. Microsoft Entra ID, Entra ID Protection, CrowdStrike, and other identity providers).
- Expert triage of suspicious sign-ins – impossible travel, atypical locations, unfamiliar devices, MFA fatigue, password spray, and leaked credentials.
- Full account takeover investigation: baseline comparison, device & IP correlation, session analysis, and lateral movement checks.
- IOC collection & hunting: IPs, device fingerprints, user agents, OAuth apps, and authentication changes.
- Containment assistance: session revocation, password resets, MFA re-enrolment, removal of malicious auth methods, account disablement (as agreed).
- Clear incident reporting with root cause, impact, and identity-hardening recommendations.

HOW IT WORKS

1. Detect: We integrate with your identity platforms and start monitoring risky users and sign-ins.
2. Triage: Our analysts quickly decide if an alert is benign, suspicious, or confirmed compromise.
3. Investigate: For true positives, we map the attack path – how the account was abused, what was accessed, and whether other accounts are at risk.
4. Contain: In line with your playbooks and approvals, we help revoke sessions, reset credentials, and remove persistence.
5. Strengthen: After each incident, we provide specific improvements for Conditional Access, MFA, privileged access and identity hygiene.

WHY ORGANISATIONS CHOOSE US

- Tool-agnostic: We work across Microsoft, CrowdStrike, and other IdPs – not just one vendor.
- Attack-centric view: We connect identity events with email, endpoint, and cloud activity to avoid tunnel vision.
- In-house feel: Your team gets direct access to analysts who know your environment and users, not a faceless queue.
- Outcome-focused: Success is not just closing an alert; it's proving the attacker has no remaining foothold in your identity layer.

Ready to get started?

Request an Identity IR Readiness Assessment:

info@smarttech247.com