Smarttech
YOUR 24/7 SECURITY PARTNER

Email Security

INCIDENT RESPONSE

Turn email from your weakest link into a contained, managed risk

Phishing, BEC, and social engineering still open the door for most intrusions. Tools like Microsoft Defender for Office 365, Proofpoint, and Abnormal Security are powerful – but alerts on their own don't close the loop.

Our Email Security Incident Response service turns these detections into fast, well-documented actions that protect users, accounts, and data.

THE CHALLENGES WE SOLVE

- Users receive suspicious emails and forward them around instead of reporting properly.
- Email security tools generate alerts, but no one has time to fully investigate the campaign.
- Credential harvesting pages are taken down slowly – after logins have already happened.
- No clear process exists to remove malicious messages from all impacted mailboxes.

WHAT YOU GET

- Triage and investigation of suspicious emails detected by O365, Proofpoint, Abnormal, and other secure email gateways.
- Deep artefact analysis: headers, infrastructure, sending IPs, domains, SPF/DKIM/DMARC, redirect chains, attachments, macros, and landing pages.
- Campaign-level view: we identify all targeted users, not just the first one who reported it.
- Click and credential tracking: we correlate URL clicks with identity anomalies and sign-in events to see who might be compromised.
- Rapid containment actions: tenant-wide message removal, sender/domain blocking, URL blocking, and indicator sharing with identity/endpoint tools.
- BEC & fraud investigation: analysis of payment-change requests, supplier impersonation, and executive spoofing patterns.
- Clear, reusable reporting your security and compliance teams can share internally.

HOW IT WORKS

1. Alert or user report: A suspicious email is detected by your tools or reported to us.
2. Email forensics: We pull artefacts, detonate attachments/URLs where needed, and classify the threat.
3. Blast radius analysis: We search for similar emails, impacted users, and evidence of engagement (clicks, replies, data sent).
4. Containment: We remove emails, block senders/domains/URLs, and trigger identity or endpoint playbooks if compromise is suspected.
5. Report and feedback: We package findings into a clear incident report and provide training insights for users and configurations.

WHY ORGANISATIONS CHOOSE US

- Multi-vendor coverage: Defender for O365, Proofpoint, Abnormal and others – we operate across your stack instead of forcing a rip-and-replace.
- Beyond “phishing”: We cover BEC, vendor fraud, internal phishing, malware campaigns, and targeted spear-phishing.
- Human + tooling: Our analysts combine automated analysis with expert judgement to reduce false positives and uncover stealthy attacks.
- User-centric: We design our approach to support user education and reduce “phish fatigue” over time.

Ready to get started?

Send us a sample suspicious email and we’ll walk you through our process

info@smarttech247.com