Smarttech
YOUR 24/7 SECURITY PARTNER

Endpoint

INCIDENT RESPONSE

The expertise you need when something bad is running on your devices

Endpoints are where attackers execute code, steal data, and move laterally. Whether you're using Microsoft Defender for Endpoint, CrowdStrike Falcon, Palo Alto Cortex XDR, or a mix, you need more than alerts—you need experts who can tell you what's actually happening and stop it quickly.

Our Endpoint Incident Response service provides that expertise on demand.

THE CHALLENGES WE SOLVE

- SOC teams get overwhelmed by EDR alerts and struggle to see the full story.
- It's hard to decide when to isolate a device vs continue investigation.
- Suspicious binaries and tools appear, but no one is sure if they're malicious, PUPs, or admin tools.
- Incidents are "closed" in tools without clear documentation or lessons learned.

WHAT YOU GET

- Full investigation of endpoint alerts across your chosen EDR/XDR platforms.
- Deep host timeline analysis: processes, parent-child relationships, command lines, registry keys, scheduled tasks, services, user activity.
- Lateral movement mapping: RDP, SMB, PSRemoting, remote WMI, credential theft behaviours and privilege escalation attempts.
- IOC and TTP cataloguing: hashes, filenames, IPs, domains, mutexes, tools, and behaviours associated with the intrusion.
- Containment actions: endpoint isolation, process termination, file quarantine, and indicator blocking (subject to agreed playbooks).
- Remediation guidance: what to clean, what to re-image, and what to monitor going forward.
- Executive-ready incident reports that non-technical stakeholders can understand.

HOW IT WORKS

1. Detection: An EDR/XDR alert fires or a suspicious device is reported.
2. Scoping: We quickly determine whether this is local noise or part of a broader incident.
3. Forensic-style investigation: Within the constraints of the EDR tool, we reconstruct the sequence of events and identify root cause.
4. Containment: Based on your risk tolerance, we isolate systems, remove malware and persistence, and block indicators.
5. Recovery roadmap: We advise on re-imaging, patching, application controls, and EDR policy adjustments.

WHY ORGANISATIONS CHOOSE US

- Multi-stack experience: Our analysts work daily with Defender, CrowdStrike, Cortex and other EDR/XDR tools.
- Clear communication: We translate low-level artefacts into concise risk statements and action plans.
- Partnership mindset: We collaborate with your internal IT and security teams rather than dictating from afar.
- Security outcome focus: Our goal isn't just "closing alerts" – it's restoring trust in your endpoint estate.

Ready to get started?

Share your EDR stack and we'll map out how we can plug in.

info@smarttech247.com