24/7 Managed Extended Detection & Response (MXDR)

Continuous detection, automated response, analyst-led containment.

Modern attacks don't keep office hours. Ekco's Managed Extended Detection & Response (MXDR) combines industry leading technology with automation and expert analysts to stop threats fast, day and night.

Ekco monitors your environment around the clock, detects real threats fast, and takes action so your team doesn't have to.

Book a 30-minute MXDR Readiness Call
Request pricing | Start a 30-day PoV

Why teams choose Ekco

- **Automation-first operations:** Automation driven playbooks accelerate triage, enrichment and response, so your team sees fewer false positives and faster containment.
- **Intelligence-enriched decisions:** Every incident is contextualised with threat intelligence for higher-fidelity actions.
- **Integration First:** Native integrations across your technology stack provide unified visibility across identities, endpoints, email and cloud workloads
- **Right-sized service levels:** Essentials / Standard / Premium tiers align to your risk profile, outcomes and reporting needs.

Powered by Microsoft Defender CROWDSTRIKE

P1 incident response target: 30 minutes
Every second counts, our average SLA is 15 minutes, but we guarantee 30 minutes.

Clear escalation and authority-to-act so we can isolate affected endpoints/ users (Microsoft or CrowdStrike) without delays, within agreed boundaries. Rapid containment reduces the impact of an attack.

Operational transparency
Real time dashboards, Monthly operational pack, Quarterly Business Review, Annual service review, covering incidents, tuning changes, ingestion/ cost, and SLA performance.

Continuous improvement
As your environment or risk profile shifts (new apps, mergers), detections and runbooks shift with it. Detection tuning and automation enhancements are part of BAU, not a separate project

info@ek.co

CREST | PEN TEST | SOC

Ekco is a European leader in managed cloud and cyber security.

We make it easier for growing organisations to innovate confidently, by securing users, devices, data and cloud services with round-the-clock expertise and pragmatic, outcome-driven operations.

With 300+ dedicated security specialists, we cover the full cyber lifecycle, prevention, detection, response and recovery. Our teams bring hard-won knowledge of how modern attacks unfold and the proven strategies and technologies to stop them, so your business keeps moving.

How it works:

1. **Connect:** We onboard your chosen platform (Microsoft or CrowdStrike) and any agreed sources.
2. **Detect & Enrich:** Analytics and use cases trigger and we enrich incidents automatically with threat
3. **Respond:** Runbooks drive consistent containment; analysts execute or guide actions with clearly audited action..
4. **Improve:** Regular reviews tune detections, automation and reporting to your changing risk.

Service options:

- **Essential:** Core telemetry onboarding (Microsoft *or* CrowdStrike), curated detection set, 24/7 alert triage, guided containment, monthly reporting.
- **Standard:** Threat-intel enrichment, automation-assisted response with enhanced identity threat detection.
- **Premium:** Proactive threat hunting, bespoke playbooks and extended detection library based and log source onboarding

info@ek.co