EKCO

> “Threats don’t sleep. Neither do we, Advanced threats need advanced cyber defence.”

24/7 Managed Extended Detection & Response (MXDR)

The cybersecurity threat landscape is constantly evolving, with cybercriminals becoming increasingly sophisticated in their tactics, techniques and procedures. Organisations of all sizes face a myriad of challenges, including advanced persistent threats, ransomware attacks, insider threats, and targeted phishing campaigns.

Attackers are leveraging emerging technologies such as artificial intelligence and machine learning to bypass traditional security measures, making threats more complex to deal with while they also grow in number. The ever-changing nature of the threat landscape makes it difficult for organisations to keep pace and adequately protect digital assets, data and infrastructure.

In this dynamic environment, the need for 24/7 detection and response becomes crucial to ensure an organisation's cybersecurity resilience. Ekco’s 24/7 Managed Extended Detection & Response (MXDR) Service helps identify threats and potential security incidents before they escalate into full-blown breaches. Through Ekco’s proactive approach to cybersecurity, organisations can minimise the impact of attacks, reduce downtime, and prevent significant financial and reputational damage.

Ekco’s 24/7 MXDR Service is essential as cybercriminals often exploit vulnerabilities outside of regular business hours, when many IT teams are off-duty. By having Ekco’s 24/7 MXDR Service in place, your organisation can effectively mitigate risks and stay one step ahead of cyber adversaries in this increasingly hostile digital landscape.

Powered by

Microsoft Sentinel
Microsoft Defender
Recorded Future
Radar®
CROWDSTRIKE
SentinelOne

24/7 Threat Protection

Cybercriminals often exploit vulnerabilities outside regular business hours. Ekco’s 24/7 MXDR service ensures continuous security coverage, protecting your systems and data from threats even when your internal IT teams are off-duty.

Extended Expertise

Ekco’s sophisticated MXDR service will give your organisation access to skilled cybersecurity leaders with extensive experience in threat detection and response, enhancing your security capabilities and providing valuable insights to help navigate the complex threat landscape.

Peace of Mind

Ekco’s Microsoft MXDR service provides 24/7 eyes on screen monitoring and real-time analysis, helping to detect and identify threats before they escalate into severe security incidents. By employing a proactive approach and staying up-to-date with the latest threat intelligence, our services help organisations build a robust security posture, effectively mitigating risks in the ever-evolving threat landscape.

Standard Offering

Ekco’s MXDR service is a proactive, metrics-driven offering. We include pre-emptive threat hunting, threat intelligence and MITRE coverage mapping as standard. We test our service annually, to demonstrate our service performance.

info@ek.co

MXDR: Beyond Detection, Proactive Threat Protection

Ekco is a leading provider of Global Security Operations Center (SOC) services, with SOC operations in the UK, Ireland the Netherlands and Malaysia. Our SOC services leverage the advanced features of our unified threat detection platforms to provide comprehensive proactive protection against cyber threats.

Our SOC is equipped with sophisticated technologies and is staffed by highly experienced cybersecurity analysts who possess the knowledge and skills to proactively detect, analyse, and respond to potential threats.

Our team can help businesses safeguard their critical assets by continuously monitoring their environment and users, identifying vulnerabilities, and providing guidance on how to mitigate risks. By partnering with Ekco for cyber security, our customers receive the highest quality cyber security expertise and services to protect their assets and reputation.

At Ekco, we understand that each organisation has unique security needs. That's why we offer tiered cybersecurity solutions designed to scale with your business. Our Standard and Premium packages build upon one another to provide a robust foundation of protection with the flexibility to expand services as your cyber maturity and resilience grow.

Standard

Round-the-clock proactive MXDR services powered by leading technologies to provide near real time response to threats.

24x7 MXDR Monitoring

A 24x7 MXDR service with eyes on screen around the clock detection and response from experienced threat experts. Allowing you to focus on other important areas of your business.

Expert Analysis & Response

Using industry-leading tooling to provide identification, analysis, investigation and containment or escalation of significant alerts and incidents.

Sophisticated Automation & AI

Integration to sophisticated SOAR platform leveraging leading AI capabilities providing near real time response to evolving threats

Threat Intelligence

Integrated Threat Intelligence feeds to continually enhance detection capability and provide real time information on external threats

Real Time Threat Hunting

Diligent surveillance of telemetry data and SOC Threat Intelligence unveils covert threats by analysing TTPs, unusual user behaviour, and network anomalies.

MXDR Dashboard

Unlock actionable insights with the Ekco Sphere MDR Portal—delivering deep security intelligence to empower strategic decision-making.

Premium

MXDR Premium offering providing enhanced capabilities and custom options to enhance Cyber maturity and resilience.

Enhanced Identity Monitoring

Enhanced Identity monitoring provided by Recorded Future to protect your business users from stolen identities and compromised credentials

Defensive Automation

Customised and proactive SOAR playbooks and automations leveraging leading AI capabilities to provide automated defensive protection and blocking from evolving cyber threats

Proactive Threat Hunting

Proactive and automated Threat Hunting tailored to the business risk ensuring there is no place to hide and providing a relentless pursuit of hidden risks.

Enhanced Threat Detection

Develop tailored use cases, detections, and analytics capabilities aligned with your business objectives—continuously refined to adapt to the ever-evolving threat landscape.

Expanded Integration

Onboard an extensive array of core and additional log sources and integrate existing security tools extending security visibility for a comprehensive and holistic view.

Insightful Reporting

Gain actionable insights with our in-depth reporting packs providing security insights and governance

Microsoft Sentinel | Radar® | Microsoft Defender | CROWDSTRIKE | SentinelOne | Recorded Future

Why Ekco MXDR Service?

100,000+
Alerts analysed per month

Holistic Coverage

- Identities
- Endpoints
- Network
- Infrastructure
- Cloud
- SaaS

Microsoft Solutions Partner
Security

Specialist
- Cloud Security
- Identity and Access Management
- Information Protection and Governance
- Threat Protection

CREST | PEN TEST | SOC

Detection Engineering

- Rapid deployment of Ekco's detection library providing rapid defensive capability
- Global detection engineering and use case library comprising 500+ Custom Analytical detections & rules
- Continual evolution, enhancement and fidelity development to detect the latest cyber threats

Proactive Threat Intelligence & Hunting

- Sophisticated Threat Intelligence Integrations using Industry and Market leading capabilities
- Managed TI services providing dark web analysis of deep industry insights and threats covering brand, credentials & Intelligence.
- Proactive and defined Threat Hunting in relentless pursuit of threats, blind spots and risks

Guided & Automated Rapid Response

- Our 24/7/365 SOC services act as an extension of your business acting as your Security Guardian giving you complete piece of mind
- 24/7 on demand access to our expert SOC Security team to provide help, guidance and advise when its needed
- Sophisticated SOAR response capability providing near real time response to threats

Next Generation Detection & Response

Ekco's MXDR Service makes it easy to collect security data across your entire hybrid organisation from devices, users, apps, servers and any cloud. Our MXDR Service is scalable and uses the power of Tines SOAR Automation with Integrated Artificial Intelligence to ensure you are identifying real threats quickly. Our MXDR service eliminates the need to spend time on setting up, maintaining and scaling infrastructure.

Integration & Holistic Visibility

Our MXDR Service is designed for dynamic environments providing holistic visibility and integration capabilities. Our SOAR platform enables rapid identification of anomalous activity and has a vast library of integrations to any existing security tooling investments making data collection fast and scalable in any infrastructure, cloud or application.

ATT&CK Alignment & Detection Maturity

Ekco's Microsoft MXDR includes a comprehensive library of over 500 curated detections, rigorously tested through real-world scenarios and adversary emulation. These detections are mapped to attacker behaviours using the MITRE ATT&CK framework—a globally recognised knowledge base of real-world adversary tactics, techniques, and procedures. This ensures we have the best detection capability and documented operating procedures to ensure threat are eradicated effectively.

Threat Intelligence

Ekco's MXDR service harnesses market leading external threat intelligence integration provided by Recorded Future, providing contextualization across events, alerts and Security Incident investigation activity providing comprehensive intelligence of real-world threats enabling our SOC Analysts to respond effectively to real world threats.

Ekco is one of Europe's leading managed cloud and cybersecurity service providers. We make it easier for you to innovate, scale, manage, troubleshoot and secure.

With a network of over 300 dedicated security specialists, we have the skills and experience to support your entire cyber security lifecycle. Our experts know the tools and methods used by the criminal underworld to successfully attack organisations across the globe. We know the strategies and technologies needed to protect you and your assets, and we have extensive knowledge on how to prepare and protect organisations from a crisis.