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 Microsoft MXDR Service is essential as cybercriminals often exploit vulnerabilities outside of regular business hours, when many Organisations' 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.

24/7 Threat Protection

Cybercriminals often exploit vulnerabilities outside regular business hours. Ekco's 24/7 Microsoft Sentinel 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 Microsoft 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 helps 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 to you annually, to demonstrate our service performance.

Powered by Microsoft Sentinel

info@ek.co

Ekco 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 Essential, Standard, or 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.

Essentials

Round-the-Clock MXDR powered by Sentinel & Defender with UEBA Integration

24x7 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.

Seamless Integration

Comprehensive deployment and onboarding for your Microsoft & Cloud ecosystems including EntraID, and Office365, with robust monitoring across Azure logs, Defender services, and cloud applications.

Expert Analysis & Response

Using Microsoft Sentinel & Defender provide Identification, analysis, investigation and containment or escalation of significant alerts and incidents.

Threat Intelligence

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

Standard

Essential offering enhanced with custom Integrations, detections and advanced threat hunting

Expanded Integration

Onboard an extensive array of core and additional log sources and integrate security tools extending beyond the Microsoft suite for a comprehensive and holistic view.

Sophisticated Threat Hunting

Diligent surveillance of telemetry data unveils covert threats by analysing TTPs, unusual user behaviour, and network anomalies, ensuring relentless pursuit of hidden risks.

Enhanced Threat Detection

Craft custom Use cases, playbooks, detections and analytics capabilities with ongoing refinement, adapting dynamically to the evolving threat landscape.

Insightful Reporting

Gain actionable insights with our in-depth reporting packs providing security insights and executive summaries to drive strategic decision-making.

Premium

Enhanced offering providing custom options to enhance Cyber maturity and resilience

Managed Threat Intelligence

Business aligned monitoring and dark web analysis of deep industry insights and threats covering brand, credentials & third-party monitoring to reduce a business risk profile.

Sophisticated Automation & AI

Design, build and deployment of advanced playbooks and custom automations, slashing incident response times providing efficiencies and amplifying your security posture and agility.

Log Storage & Cost Optimisation

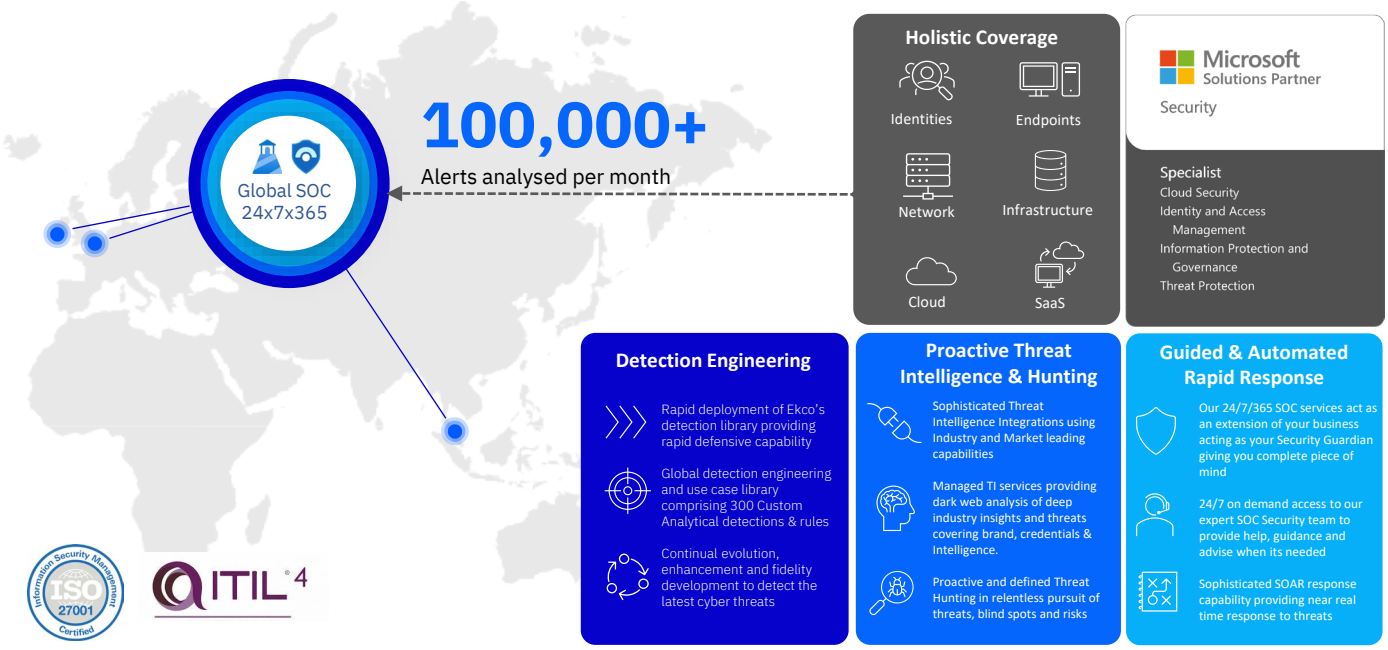
Optimise log source and data storage through data transformation providing peak efficiency and cost-effective ingestion and storage strategies to minimise costs.

Incident Response

Incident response retainer providing preparation, rehearsal and immediate cyber incident response capability to contain, eradicate, and recover from a Cyber Incident

info@ek.co

Why Ekco MXDR Service?



Next Generation Detection & Response

Ekco Microsoft MXDR makes it easy to collect security data across your entire hybrid organisation from devices, users, apps, servers and any cloud. Microsoft Sentinel is infinitely scalable and uses the power of Microsoft artificial intelligence tracking over 65 trillion signals daily to ensure you are identifying real threats quickly. Our cloud native service eliminates the need to spend time on setting up, maintaining and scaling infrastructure.

ATT&CK Alignment & Detection Maturity

Ekco's Microsoft MXDR comes complete with a vast library consisting of 300+ curated detections tested under real world and adversarial emulation mapped to attacker behaviors and the MITRE ATT&CK framework, an open globally accessible knowledge base of real-world adversary tactics and techniques and procedures. This ensures we have the best detection capability and documented operating procedures to ensure threat are eradicated effectively.

Integration & Holistic Visibility

Our Microsoft MDR Platform is designed for dynamic environments. Our platform enables rapid identification of anomalous activity and has a vast library integrations to any existing security tooling investments making data collection fast and scalable in any infrastructure, cloud or application.

Threat Intelligence

Ekco's Microsoft MXDR Sentinel service harnesses multiple external live threat intelligence integrations, 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 cyber security 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.

info@ek.co