

Graphnet Health

Trust in Every Record , Modernising Cyber Defence for Critical Healthcare Systems

Case Study



Overview

Graphnet Health is the UK's leading provider of shared care record and population health solutions, delivering integrated data systems that improve patient outcomes across health and social care. With around 300 users and a large Microsoft Azure footprint, Graphnet's platform is central to healthcare delivery across the country.

The healthcare technology sector faces acute cyber security challenges. As data privacy regulations tighten and digital patient records become the norm, providers must safeguard vast volumes of sensitive health information while navigating a growing threat landscape. For organisations like Graphnet, ensuring compliance, maintaining data integrity and defending against evolving cyber risks are critical to delivering safe, trusted care.



Challenge

Graphnet Health had previously engaged a Managed Security Provider (MSSP) to deliver a 24x7 SOC service, but it fell short of expectations, resulting in a consequential loss of confidence in the service.

Additional challenges included:

- The scale and complexity of the Microsoft Azure environment.
- A high volume of activity across cloud workloads.
- The need to preserve and migrate existing security playbooks developed in-house.

Graphnet needed more than monitoring — they required a true managed detection and response (MDR) partner capable of being highly proactive by managing and remediating threats with precision and minimal internal overhead.



At a Glance

Customer:
Graphnet

Organisation Size:
250-500

Industry: Healthcare

Solutions:
MDR as a Service | Assure 365

Products: Microsoft
Sentinel, Microsoft Azure



Solution

Following a comprehensive market review and tender process, CyberOne was selected to transition Graphnet to a fully managed MDR service powered by Microsoft Sentinel.

CyberOne's CREST-certified SOC team initiated a detailed transition programme, including:

- An audit of the existing Microsoft Sentinel environment.
- Migration and optimisation of Graphnet's playbooks.
- Development of new playbooks aligned to MITRE ATT&CK.

As part of the engagement, CyberOne introduced its proprietary tooling to enhance security operations and drive greater efficiency. This included **IRIS**, an AI-powered automation engine that enables real-time alert triage and dramatically reduces noise for analysts; **Hyperion**, a continuously developed rulebook containing over 1,000 custom detection rules designed to rapidly uplift threat coverage and align with MITRE ATT&CK and **Athena**, a powerful threat intelligence programme that strengthens detection and supports proactive threat hunting. Together, these tools deliver smarter, faster and more scalable security outcomes.



Results

By partnering with CyberOne, Graphnet transformed its cyber security operations—shifting from reactive alert handling to a proactive, intelligence-led approach. The benefits were immediate and measurable:

- **Immediate Reduction in Internal Workload**
CyberOne's SOC filtered and actioned the noise, significantly reducing the number of alerts requiring Graphnet's attention.
- **Improved Security Posture**
Comprehensive SOC and MDR services significantly strengthened cyber security, ensuring robust protection across Graphnet's operations.
- **Reduced Risk of Breaches**
The integrated MDR service actively monitors, investigates and mitigates threats in real time, significantly lowering the risk of breaches and strengthening Graphnet's overall security posture.
- **Enhanced Compliance Posture**
Continuous monitoring and tailored reporting ensured ongoing alignment with healthcare regulations.
- **Improved Threat Detection and Response**
Real-time triage and advanced analytics enabled faster threat containment, streamlined investigation and vastly improved incident resolution across the environment.
- **Future-Proofed Security with Assure 365**
The modular platform, powered by Microsoft Sentinel and enhanced by CyberOne's proprietary technologies, provides a scalable foundation that evolves with Graphnet's growth and the ever-changing threat landscape.

This comprehensive solution delivered by CyberOne has equipped Graphnet with a resilient, scalable and intelligence-driven security framework that reduces operational burdens, enhances compliance and enables secure, sustainable growth in a highly regulated healthcare environment.



After moving our Managed Detection & Response service to CyberOne's SOC, we immediately saw a significant and tangible improvement in both the quality and responsiveness of the service. The engagement from CyberOne's team was a step change from our previous experience—proactive, knowledgeable and truly embedded into our operations.

One of the biggest benefits was the dramatic reduction in alert fatigue. Our internal team no longer had to sift through hundreds of alerts every month. Instead, we now receive only a small number of high-priority, actionable notifications, which has allowed us to focus on strategic security improvements rather than day-to-day firefighting.

Information Security Manager, Graphnet

About CyberOne

A Microsoft Security Elite Partner and member of the Microsoft Intelligent Security Association (MISA), delivering world-class AI-augmented Managed Extended Detection & Response (MXDR) services. Our Microsoft-verified Managed XDR solution combines Microsoft's security platform with CyberOne's accredited experts to help organisations prevent, detect and respond to modern cyber threats faster while accelerating cyber maturity and maximising Microsoft investments.

Through our 24x7x365 Global Security & Network Operations Centre (SNOC), CyberOne provides continuous protection supported by NCSC-accredited Cyber Incident Exercising and Response, CREST-accredited SOC services and Penetration Testing, alongside clear, measurable service level agreements (SLAs). CyberOne's Consulting, Professional and Managed Security services help organisations protect critical operations, strengthen compliance and move confidently from cyber risk to cyber resilience.



+44 (0) 3452 757575

hello@cyberone.security

cyberone.security

