DARKTRACE

CASE STUDY

Milton Keynes University Hospital

NHS
Milton Keynes University Hospital
NHS Foundation Trust

Overview

Industry

- Healthcare and Pharma

Challenge

- Lean security team faced with overwhelming number of alerts
- Lack of visibility into dynamic workforce
- Need for continuous operational abilities

Results

- 24/7 AI Autonomous Response
- Major vulnerabilities detected and remediated with Cyber AI
- Surgical defense against attacks
- Team left with more time for digital transformation projects

Business Background

Founded in 1984, Milton Keynes University Hospital serves the local citizens of Milton Keynes, as well as the wider communities of Buckingham, Bedford, and Northampton. With the hospital's research and development work, training program for undergraduate medical students, and use of innovative IoT technology, maintaining the integrity of its digital infrastructure while undergoing various technological transformation projects has been a priority.

> I am confident that we will be in a much better place to fend off another serious cyber-attack on the NHS with Darktrace at work.
>
> **Craig York, CTO, Milton Keynes Hospital**

Challenge

In early 2020, the coronavirus pandemic highlighted the true necessity of the healthcare sector – and demonstrated that downtime simply isn't an option. Day-to-day, medical staff rely on digital systems to keep them going, and security teams in turn require robust cyber defenses to maintain the integrity of their digital environments.

Craig York, CTO at Milton Keynes University Hospital NHS Foundation Trust, recognized the need for a forward-thinking approach to cyber security. Putting patient care at the top of the agenda, York sought a technology which fights back against threats as they emerge, taking autonomous action to protect sensitive data and defend the integrity of the hospital's systems. And with his lean security team, he needed a solution that cuts through the noise, triaging alerts as they arise.

After the WannaCry ransomware attack on NHS systems in 2017, the need for cyber defenses that could take action before the damage was done became truly apparent, and security solutions that can autonomously neutralize emerging threats became a necessity.

Solution

To address these concerns, Milton Keynes University Hospital looked to a solution deployed by a fellow NHS trust – Darktrace's AI, which had detected and contained WannaCry within minutes of it emerging.

Analogous to the human immune system, Darktrace's AI works by learning the 'pattern of life' for every hospital user, device, and container. Such an understanding of what normal looks like enables it to detect even the most subtle deviations indicative of threat – from low and slow attacks, to never-before-seen strains of ransomware. Thus, unlike traditional legacy tools which spot known attacks, Darktrace's unique approach catches novel threats before they do damage. And, with its autonomous response module Antigena, Darktrace's AI fights back at machine speed to neutralize all malicious behavior as and when it emerges.

> Autonomous response is the future for defending against fast-moving and unpredictable threats, before they do damage. Darktrace fights backs on our behalf so we can focus on strategic tasks.
>
> **Craig York, CTO, Milton Keynes Hospital**

Understanding emerging threats wherever they arise across cloud, SaaS, email, and traditional network environments, Darktrace's AI defends hospital systems more comprehensively than any other tool can. Correlating a number of weak indicators of potential compromise across the entire dynamic workforce, the AI's evolving understanding of 'self' for each aspect of hospital life means its detection and response capabilities are always current, and that only legitimate threats are flagged to security teams. Operative 24/7, the hospital's systems are continually protected, no matter the time of day or night.

Benefits

The value of Darktrace's technology was instantly recognized by the team at Milton Keynes University Hospital for both its ability to identify novel threats and vulnerabilities as well as its function as a force multiplier – augmenting the capabilities of the existing security professionals.

For Craig York, this technology has been a game-changer. "Having Darktrace's AI watching over your network is really just another pair of eyes, one that never sleeps and takes action in seconds to protect every digital asset you have."

With his lean security team, York has found Darktrace's ability to fight back on its behalf invaluable. And as attacks increasingly occur at machine speed, having a tool which neutralizes such threats seconds after they arise ensures the integrity of hospital systems and crucially, prevents downtime.

Darktrace's AI shines a light into hard-to-track places, giving Milton Keynes Hospital's security team visibility into its entire dynamic workforce. The team has gone from fire-fighting and alert fatigue, to being able to plan digital transformation projects, increase adoption of state-of-the-art technology, and trial innovative medical technological developments.

In the event of an attack, Darktrace's AI surgically intervenes, inhibiting the illegitimate activity alone – allowing normal business practices to continue as normal. This means that even the infected device can continue to undertake its usual actions, just not malicious ones, so no change is seen in the day-to-day business.

Now more than ever, self-learning AI is critical to the task of ensuring the operational continuity of hospital systems. Workers at Milton Keynes Hospital depend on it.

> At Milton Keynes University Hospital, Darktrace's AI is fundamental in helping us defend our network against cyber-attacks.
>
> **Craig York, CTO, Milton Keynes Hospital**

Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com