

# KTR Systems

For over fifty years, KTR Systems has been a leading manufacturer of high-grade power transmission components for mechanical and plant engineering.



## At a Glance

- Targeted by sophisticated email impersonation and spear phishing attacks
- Finite human IT resources facing cyber-attacks around the clock
- Limited visibility across global workforce activity

**“After being targeted with CEO fraud twice, it became extremely clear that we needed to do something about email security.”**

Head of IT and Organization,  
KTR Systems

## How Traditional Defenses Let Major Threats Slip Through

As a global company with over 1,200 employees and 24 subsidiaries, KTR Systems has a diverse and complex digital infrastructure to protect. With increasingly subtle and sophisticated cyber-attacks targeting every corner of the digital ecosystem, the IT team sought a new approach that could detect and autonomously respond to these threats. According to Olaf Korbanek, Head of IT and Organization, KTR Systems, “With traditional tools that look for signs of a threat based on historical data, you are always one step behind. These signature-based defenses are ineffective in the face of novel attacks.”

In 2019, two separate instances of CEO fraud at the company confirmed fears that their traditional security tools were unable to spot advanced and novel threats using static rules and signatures. After reporting the attacks to the authorities, Korbanek was even wrongly identified as a primary suspect in the police investigation following initial concerns of insider threat.

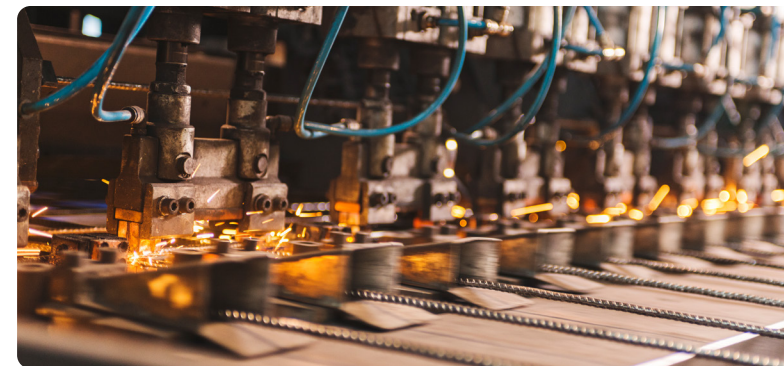
While dealing with the fallout from CEO fraud, the organization suffered another attack two months later – this time an attempted ransomware attack that originated with a phishing email. The team identified the threat before it could escalate and suffered no damage. However, by now it had become clear the team needed a robust solution to enable them to respond to email attacks 24/7.

## The Need for Autonomous Cyber Security

As a result, KTR Systems turned to Darktrace’s Immune System to defend its vast digital ecosystem. Using self-learning Cyber AI, Darktrace immediately began learning the normal ‘patterns of life’ for every user and device in the organization. By continuously revising its understanding in light of changing behavior, the AI can spot anomalous activity indicative of threat, including novel strains of malware and subtle insiders that static rules and signature-based tools are unable to detect.

**“We needed a clever approach; something to automate our processes.”**

Head of IT and Organization,  
KTR Systems



Darktrace's Cyber AI has proven especially valuable in extending and uplifting the company's overwhelmed security team, freeing them up to focus on strategic tasks. The Immune System's open architecture enables seamless integrations with disjointed defenses, streamlining alerts for the IT security team and instantly correlating insights across multiple siloes. "Darktrace's AI approach is something that I think every company should be using," states Korbanek.

---

**"Traditional security approaches are predictable for cyber-criminals. Artificial intelligence helps you to adapt to changing user behaviours."**

Head of IT and Organization, KTR Systems



## Thwarting a Zero-Day Attack With AI

The importance of Darktrace's self-learning capabilities was truly realized when KTR Systems was hit by a zero-day attack. Soon after extending Cyber AI protection to the email realm using Antigena Email, KTR Systems was targeted by a machine-speed cyber-attack. Leveraging Autonomous Response technology, Antigena Email detected and stopped the threat with rapid, targeted action.

Korbanek states "It was another situation in which Darktrace proved its value because all suspicious activity was stopped before any damage could happen." Antigena Email works by understanding the human behind the keyboard, analyzing emails in context to form a nuanced and continually evolving understanding of communication across the business. It detects subtle deviations indicative of a cyber-threat that traditional tools miss and autonomously reacts in real time, allowing normal business interactions to continue uninterrupted.

With Darktrace Cyber AI, KTR Systems is secure in the knowledge that they have complete visibility and 24/7 autonomous protection across their vast digital ecosystem.

---




**"Darktrace's AI approach is something that I think every company should be using."**

Head of IT and Organization, KTR Systems



**Darktrace's user interface, the Threat Visualizer, provides real-time visibility across the entire digital ecosystem**

### For More Information

-  [Book a free trial](#)
-  [Read the Immune System White Paper](#)
-  [Visit our YouTube channel](#)