Customer Case Study

Mercury Engineering Builds a Safer Supply Chain with Human Behaviour AI

Leading European engineering and construction firm protects its clients and reputation with a solution that stops VEC attacks.

Industry
Construction

Headquarters
Dublin, Ireland

Protected Mailboxes
2,400+

Mercury builds and manages complex engineering and construction projects for the world's leading corporations across the data centre, life sciences, and semiconductor sectors. What began as a two-man electrical firm in a Dublin apartment in 1972 has grown into an international operation with projects spanning more than 16 countries throughout Europe. Mercury offers a broad range of engineering and safety services—including offsite assembly—backed by a strong reputation for security.

The Mercury Email Security Challenge

With high-profile clients investing in large, specialised construction projects, Mercury takes data security seriously. "We're ISO 27001:2022 certified, and that's quite important to our clients," said Adam Hoffmann, IT Operations Manager. "Without it, we might not be allowed to participate in a tender."

Hoffmann and his team must also balance security against the need to work with thousands of vendors. "Our primary concern before Abnormal AI was the varying levels of cyber security maturity in the supply chain," he added. Even with Microsoft 365 security tools and a SEG, Hoffmann was seeing supply chain compromise and impersonation attacks reaching user inboxes, potentially exposing the organisation to costly consequences.

Customer Key Challenges

- Detect and stop advanced VEC attacks designed to evade M365 and the SEG.
- Maintain effective security across a large supply chain and workforce.
- Save SOC analyst time whilst reinforcing workforce security awareness.

Abnormal Solution

- Learns normal vendor behaviour to quickly detect indicators of compromise, even from trusted domains or in ongoing conversations.
- Analyses thousands of behavioural, identity, and other signals to spot attack indicators in inbound, ongoing, and internal messages.
- Automates email report investigation and response to save analyst time and give users faster, more detailed security feedback.

"Before Abnormal, we had experienced some sophisticated invoice and vendor fraud attacks getting past our native email security and SEG. Straight away in the POV, Abnormal identified these types of attacks. We saw that Abnormal was the ideal solution to address this challenge."

Adam Hoffmann
IT Operations Manager

Customer Case Study

€200K+
Total value of attempted vendor fraud during POV

90
Analyst hours saved monthly by reporting automation

44,573
Advanced attacks prevented since implementation

The Abnormal AI Solution

Hoffmann wanted a solution to stop advanced attacks. A technology partner recommended Abnormal's behavioural AI and API-based design, but Hoffmann was sceptical until the POV changed his mind.

“Abnormal found an invoice fraud attack from a lookalike domain. This wasn’t a generic approach. This group targeted our suppliers, registered a domain, compromised mailboxes, and searched for threads with unpaid invoices to latch onto,” Hoffmann recalled. Abnormal detected advanced attacks worth “hundreds of thousands of euro,” Hoffmann said. For a presentation to the CFO, “I just had one slide showing the invoice fraud that Abnormal stopped.”

Why Mercury Engineering Chose Abnormal

Abnormal enabled Hoffmann to remove redundant SEG modules. “We dialled back internal email protection and remediations because Abnormal overlaps and is easier to use,” Hoffmann said. Abnormal’s VEC detection helps Mercury protect its supply chain. Hoffmann's team blocks compromised vendors, notifies them of the incident, and outlines the security steps required to regain access.

Abnormal's AI Security Mailbox saves Hoffmann's team 90 hours monthly by automating email report investigation and remediation. AISM also encourages user reports, Hoffmann said. "We emphasise reporting suspicious emails, but without time to analyse them, that defeated the purpose," he said.“We’ve seen a significant uptake in reporting. Phishing simulations reporting rates are up to 50%.”

Constructing a Future-Proof Security Relationship

Hoffmann appreciates the responsiveness of Abnormal’s customer success team. “Any feedback we provide gets taken on board, and we see changes,” he said. He also sees Abnormal as a partner in fighting the evolution of AI-enhanced threats. “Email attacks will become even more difficult to detect because the offensive tools are becoming more sophisticated. Even just one person can orchestrate attacks at scale,” he said. “Better AI tools can assist in detecting and protecting us from these kinds of attacks. Abnormal provides that core service for us.”

> “Abnormal was so easy to set up. The beauty of its API is that you're not taking risks by introducing something inline with your email traffic, and you don't have to make any changes to your SPF. Abnormal gave us the advanced security we needed without disrupting our email operations.”
>
> Adam Hoffmann
> IT Operations Manager

Abnormal Products in use:

- Inbound Email Security
- Account Takeover Protection
- AI Security Mailbox

abnormal.ai ›

Abnormal