SOC Case Study:

LoughTec
IT • CYBER SECURITY

LoughTec Security Operations Centre stops hack on well known NI-based Contractor on day 1

The construction sector has become a serious target for cyber criminals over the last 5 years. A list of the 'known' victims of cybercrime reads like a 'Who's Who' of Irish construction. Many of the larger organisations across the country have been victims of phishing attacks, data breaches and malware attacks.

As a relatively late adapter to technology and digitisation, construction companies offer any number of breach points to cyber criminals throughout the three stages of design, construction and handover.

LoughTec has been working with several large construction companies across the island of Ireland and GB for almost 10 years, helping to protect their networks, systems and infrastructure from cybercrime.

This experience proved to be vital following an initial discussion with a major NI-based contractor around their cyber security defence posture.

The Challenge

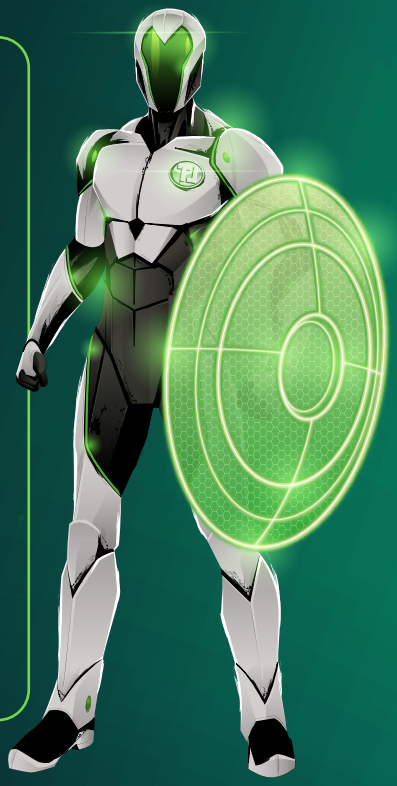
LoughTec met with this large-scale contractor to discuss their overall IT infrastructure and cyber security, and their plans to improve their defences as the business grew.

On many occasions, the biggest challenge for any cyber security company is to convince prospects and customers that they are vulnerable and under constant threat from cyber criminals.

The thought that *"It will never happen to us"* shouldn't be a reason to ignore your security posture, yet often it does. Given the scale of the contractor's operations, their workforce and their growing order book of major projects, LoughTec felt the business was particularly at risk of sophisticated cyber attacks.

It was only several weeks previous that a multi-hundred million contractor based in Belfast, had fallen victim to a ransomware attack, targeted by the same group behind the attack on Royal Mail in January 2023.

LoughTec discussed and recommended its Security Operations Centre (SOC) to the contractor, to detect, analyse and respond to cyber incidents in real-time, 24/7/365.



The Solution

Following initial discussions, the contractor made the swift decision to deploy and implement the LoughTec Security Operations Centre across the company's network and endpoints.

What is SOC?

The SOC is focused on catching breaches and rapidly responding to contain them, monitoring networks and detaining advanced threats before they can spread laterally.

It combines state-of-the-art software and cyber security professionals, working together in unison to give all businesses world-class protection from the growing cyber threat, 24/7/365.

Loughtec.com

T: +44 (0)28 8225 2445 E: info@LoughTec.com

LoughTec
IT • CYBER SECURITY

During the initial implementation of the SOC on day 1

LoughTec identified that the construction business in question had already been breached by cybercriminals. The hacker who carried out the attack had been conducting reconnaissance for quite some time, most likely collecting vital information on the business's networks, overall infrastructure, details on its employees and suppliers to identify opportunities to monetise.

The implementation of LoughTec's Security Operations Centre on day 1 was luckily coincidental with the hacker planning to launch ransomware, similar to that mentioned previously, which affected Royal Mail and Lagan SCG. LoughTec Security Operations Centre and its team of cyber engineers were able to see immediately that the hacker placed an Asian timezone on the contractor's servers, and was preparing to 'tombstone' its operations with a full ransomware lock-out.

This vital intervention prevented any cyber breach from taking place, thus saving the company's confidential intellectual property from extraction and encryption, as well as any subsequent business disruption and likely large financial ransom demand that would have certainly followed.

In summary, business continuity was ensured, a costly ransom demand, in the hundreds of thousands of pounds, was avoided in the process whilst also protecting the company's vital business reputation.

LoughTec's Security Operations Centre provides any business with:

- Active threat hunting and real-time responses, stopping cyber breaches in their tracks.
- Continuous monitoring 24/7/365 from a dedicated team of experienced cyber professionals.
- Nation-state grade managed detection and response (MDR) technology helps detect what others miss.
- Peace of mind through monthly reporting with detailed system analytics.

This business was thankful they made a swift decision to deploy the SOC based on LoughTec's advice, saving their data, reputation and finances. The business continues to be protected 24/7/365.

LoughTec currently provides cyber security solutions and managed IT services to businesses and organisations of all shapes and sizes throughout Ireland and beyond.

If you have any questions regarding the security posture for your business, please get in touch via phone, email or our website.

Loughtec.com

T: +44 (0)28 8225 2445 E: info@LoughTec.com