TALAN

Positive innovation

Talan successfully delivered **bespoke weekly threat reports** for an electricity provider in order to protect them in an **increasingly tense landscape**.

THE CHALLENGE

The client is part of the United Kingdom's Critical National Infrastructure (CNI) operating a distribution network that provides electricity to over 910,000 customers. They required a solution that could deliver reliable, timely and actionable cyber threat intelligence to help them influence their policy making, vulnerability management and reaction to upcoming and ongoing threats.

Being part of the UK's CNI the client was aware of the increasing threats to them and the specific threats that could target the energy sector. They received threat updates from the NCSC and occasionally from their managed service provider, but these reports were generic and wide-ranging. The client required something that was specific to them, the technologies they use and the sector they and their parent organisation operate in.

Recent world events have shown that CNI, specifically energy networks, are considered high value targets for malicious threat actors.

Many threat groups globally are directly funded or at least linked with hostile states, giving them increased capability and motivation.

The client's aim was to safeguard themselves against current and future threats and attacks that could affect their operational ability, the confidentiality, integrity and availability of their systems and data, and their reputation.

The client required focus on three main areas of interest:

- Attacks on CNI targets, especially those in the energy market or the UK
- Vulnerabilities listed for their extensive technology stack, including guidance on remediation.
- Attacks or threats to their Supply Chain and impacts to the client and their parent company's reputation.

THE SOLUTION

After being approached by the client, Talan created and delivered weekly threat reports these main areas:

Sector and Region-specific intelligence – CNI and energy related intelligence while reporting on cyber-attacks in the UK, including subject matter expert commentary, analysis, and recommendations.

Technology Stack vulnerability intelligence – providing the client with the latest vulnerability alerts for the versions of technology that they are using business-wide, with up-to-date vendor and patching advice.

Extended Supply Chain monitoring – including findings of real time monitoring of the client's supply chain for vulnerabilities, cyber incidents (including ransomware), data breaches and credential leaks.

Social Media and Brand – covering all forms of mainstream social media platforms as well as instant messaging and forums. Digital profiling and real-time anonymous sentiment analysis.

In addition to the delivery of these weekly reports, the service includes:

- 24/7 alerts monitoring (client is notified in real time on credential leaks, data leaks, supply chain compromises)
- Weekly editorials that include trend analysis
- Monthly touchpoints where the client can tweak/add/remove search parameters
- Monthly updates at their security forum in order to update stakeholders on cyber risks and mitigations.

THE IMPACT

The client has enhanced their security posture and awareness by actioning the weekly intelligence reports that we have provided.

Further benefits that have resulted include:

- They have ensured that their managed service provider updated and improved their patching scheduling as the client was fully aware of their technology stack vulnerabilities.
- Implementation of security measures to combat known threats and vulnerabilities.
- The ability to investigate credential leaks that they have had and have passed on intelligence to their parent company.
- Awareness throughout the organisation has been raised and the intelligence has been used to enhance business cases.