TALAN

Positive innovation

Talan was commissioned to undertake an **in-depth cyber analysis** of the current UK and global **cyber threat landscape** in order to better understand the risks faced by the UK energy sector and to inform and shape their **annual risk assessment**.

THE CHALLENGE

The client is part of a UK Critical National Infrastructure (CNI) regulatory board that oversees, reviews and advises nationally on security arrangements and policy.

As a regulatory board with a focus on CNI security, our client was aware of the increasing, specific threats that target the energy sector. They are responsible for conducting an annual risk assessment which they use to inform policy and security requirements. It was important to them to gain a full understanding of threat trends. They further required full subject matter expert analysis of these threats.

The UK's CNI has never been under more threat. Whether it is criminal organisations wanting to exploit the data that they hold, or the looming threat of state sponsored activity, it continues to be a prized target.

Their aim was to produce public-facing guidance documents and assurance frameworks as well as research reports for future technologies that are likely to impact transportation and associated supporting systems.

Our client wanted to ensure the following key areas of interest were covered within the report:

- **Trends and incidents, particularly relating to the UK energy sector**
- **Changes to the threat landscape in the past 12 months**
- **Identification of the main threat actors by type, location, and nature of attack**
- **Knowledge of victims subject to attack and the nature of attacks**

THE SOLUTION

For this engagement, Talan developed comprehensive analytical cyber threat report into the threats facing the UK energy sector.

The report was timely and actionable, providing a detailed analysis of cyber threats specific the energy sector and systems used. Trend analysis and a clear and concise presentation of the threat landscape, including indicators of compromise (IOCs) was presented. Additionally, the report provided recommendations and mitigations based on Talan's subject matter expertise and industry best practices.

Our approach involved the collection and analyses in real-time include Open Web, Deep Web, and Dark Web content. The Dark Web content spans a wide range of onion sites: illegal marketplaces, paste sites, hacker forums and more. Other sources included paste bins, blogs and forums, and news outlets.

Using this source material we were able to break the report down into these clear and logical section and focused sub-sections.

Key Threat Actors

- Nation State and State Sponsored
- Insiders
- Cybercrime
- Hacktivist
- Opportunistic Threat Actors
- Key Threat Actors targeting the Energy Sector

Key Attack Vectors

- Social Engineering
- Technical analysis using MITRE ATT&CK

Threat Targets

- Cloud
- Internet of Things, Operational Technology, and Supervisory Control and Data Acquisition

Emerging Technologies Risks

- Artificial Intelligence and Ethics
- Deepfakes

THE IMPACT

Using the analysis and information provided in the Talan report, our client was able to refine and update its annual sector risk assessment. The final report for the client was based on the evolving threat landscape, technological advancements, and lessons learned from previous cyber incidents.

The report strengthened the client's understanding of the threat landscape, which allowed them to inform their regulatory policies with measures that remain effective and adaptive in the face of emerging cyber threats.

Further positive impacts included:

Regulatory Compliance Enforcement - We helped the client to ensure that regulatory frameworks are aligned with the current threat landscape and promote effective cybersecurity practices.

Risk Assessment and Management - We enabled the client to conduct an effective risk assessment and develop risk management strategies to safeguard the future of its critical energy infrastructure.

Resource Allocation Optimisation - Using insights from the report, the client allocated resources more effectively and added targeted measures to address specific threats throughout the sector.

Public Confidence and Trust - Demonstrating a proactive stance against cyber threats through regular threat reports enhances our client's stakeholder confidence and trust.

Collaboration - Our client may share the threat intelligence with UK energy companies and other stakeholders, allowing them to foster collaboration.

With our clients we are delivering bespoke threat protection.

www.talan.com