TALAN

Positive innovation

Talan was engaged to evaluate **current and future cyber threats** targeting critical national infrastructure to inform the **defence strategy** for a client.

THE CHALLENGE

A leading energy provider in the UK, classified as critical national infrastructure (CNI), faced escalating cybersecurity threats amid growing geopolitical tensions and the increasing sophistication of cybercriminals.

The energy sector's reliance on digital technologies and interconnected systems exposes it to vulnerabilities that could be exploited to disrupt national energy supply, endanger public safety, and cause significant economic losses.

The primary task was to develop and implement a robust cyber threat intelligence framework.

This would enable the energy provider to:

- Identify and assess emerging cyber threats and vulnerabilities specific to the energy sector.
- Monitor threat actors and activities targeting CNI globally.
- Enhance the cybersecurity posture of the energy infrastructure through actionable intelligence.
- Facilitate collaboration with national cybersecurity agencies and other energy sector entities for information sharing and joint threat mitigation efforts.

THE SOLUTION

A multidisciplinary team of Open-Source Intelligence (OSINT) analysts, cybersecurity experts, and sector specialists was formed to undertake the following:

Cyber-Physical Threat Landscape Mapping: Used advanced OSINT techniques to map out the threat landscape targeting SCADA, OT, and CPS; identifying patterns, techniques, and potential vulnerabilities.

Sector-Specific Threat Landscape Analysis: Conducted a comprehensive analysis of the cyber threat landscape specific to the energy sector, using OSINT to identify trends, tactics, techniques, and procedures (TTPs).

Threat Modelling: Leveraged the MITRE ATT&CK framework to identify and prioritise potential threat actors and their likely objectives.

Infrastructure Vulnerability Scanning: Used advanced tools to scan the digital footprint of the energy infrastructure, identifying exploitable vulnerabilities in software, hardware, and networks.

Gap Analysis: By mapping its existing security controls against the TTP's listed in the MITRE ATT&CK framework, the energy supplier was able to identify gaps in its defences where additional controls or improvements were needed.

Threat Actor Profiling: Monitored and profiled threat actors known for targeting CNI, using OSINT to gather intelligence on their methodologies, motives, and potential targets.

Collaborative Intelligence Sharing: Established secure channels for intelligence sharing with national cybersecurity agencies, industry partners, and international organisations specialising in energy sector security.

Customised Intelligence Reporting: Developed tailored intelligence reports providing actionable recommendations for mitigating identified threats and vulnerabilities, prioritising actions based on risk levels.

THE IMPACT

The implementation of Talan's comprehensive cyber threat intelligence strategy created:

Enhanced Threat Visibility: The energy provider achieved a significant enhancement in visibility into emerging cyber threats, with an 80% increase in the early detection of potential cyber incidents.

Proactive Risk Management: Actionable intelligence enabled a shift from reactive to proactive risk management, with a 50% reduction in the incidence of successful cyber-attacks within the first year.

Strengthened Resilience: Through targeted vulnerability remediation and enhanced defensive measures informed by OSINT findings.

Strategic Collaboration: The establishment of intelligence-sharing partnerships led to improved coordination in national cyber threat response efforts, elevating the collective defence posture of the UK's critical national infrastructure.

By leveraging OSINT to gain advanced insights into potential threats and vulnerabilities, our client not only enhanced its cybersecurity defences but also contributed to the national security and economic stability of the country.

The proactive and collaborative approach adopted in this strategy serves as a model for other CNI sectors aiming to mitigate the evolving landscape of cyber threats.