Gemserv
A Talan Company

Gemserv created a cyber threat intelligence campaign for a consultancy client, empowering them to produce robust guidance for numerous industries.

THE CHALLENGE

The client, a professional consultancy organisation, was commissioned to deliver cyber services to improve understanding and resilience of cyber security within the UK transportation sector. This sector is an attractive target for malicious and disruptive cyber-attacks. As the industry increases its use of digitalisation and interconnectivity, the risk to exploitation also increases.

The client required actionable cyber threat intelligence feeds and insights to assist with the evaluation of historic, current, and upcoming threats and risks within both sectors, as well as any other sectors in which similar infrastructure and technologies are deployed. 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 supporting systems.

The client articulated they had three critical use cases:

- Reports of current and past attacks across the two sectors, including any supply chain-related intelligence relevant to the sectors.

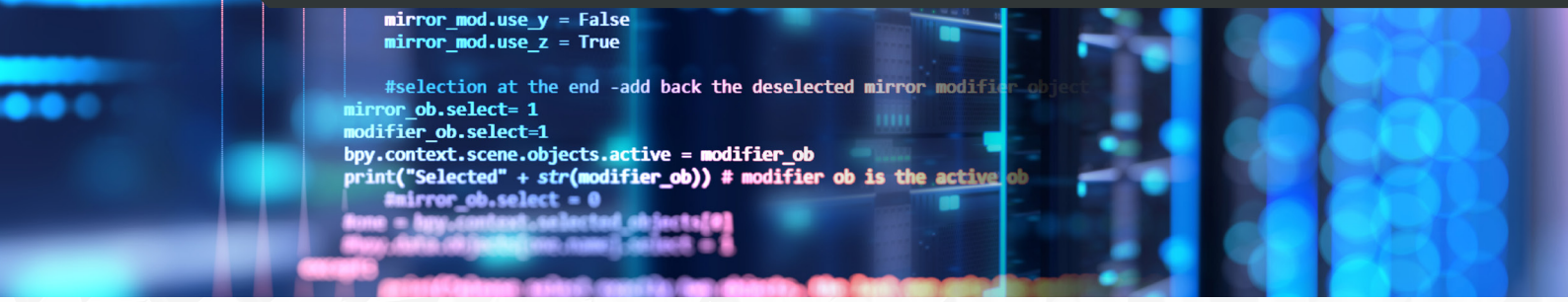
- Analysis on emerging threats and attacks across the same vertical, including Proof of Concept examples, research and whitepapers. This includes the potential exploitation of new technologies, such as Generative AI.

- Investigation of other verticals of interest, for example the analysis of vulnerabilities and exploits on common technology and/or infrastructure, which could be leveraged to carry out attacks. This analysis is extremely useful to understand what risks may be coming in the near future for any particular sector.

With our clients we are delivering bespoke threat protection.
Find out more here

Contact Us:
BD@gemserv.com

Gemserv®
A Talan Company



THE SOLUTION

For this engagement, Gemserv developed and delivered a comprehensive cybersecurity intelligence plan in the form of weekly reporting and investigations as well as supporting on ad-hoc requests from the client for time-critical updates.

Each week consisted of themes for investigation, provided by the client and enhanced by our consultants, with the engagement spanning from research on physical systems (IoT, OT/SCADA) to threat actors (insider threats, nation-state activity) to Cloud and IT infrastructure.

The weekly reports explored both up-to-date reports as well as historic incidents, in addition to emerging threats and vulnerabilities in areas such as Machine Learning and AI technologies. We also supported the client with the analysis of specific topics and/or incidents of interest.

Our analysts were able to provide detailed insights and rationale behind several threat groups' attack methods and operations to help accurately predict their 'next move' and in turn protect the sectors' critical infrastructure by implementing targeted mitigations.

Our experts carried out monitoring across several different domains, using our Threat Intelligence platform combined with experienced analysts' guidance. The domains included (but were not limited to):

- Sector and Region specific activity
- Supply-chain security analysis
- Evaluation of Proof-of-Concept exploits, whitepapers, and academic research
- Emerging threats associated with physical and non-physical systems
- Geopolitical Intelligence, including insights into potential conflict-related repercussions.

THE IMPACT

The client significantly enhanced their ability to produce high-quality and comprehensive public-facing guidance documents, assurance frameworks, and research reports aimed at improving any sector's cyber posture.

Additionally, the integration of reports from other verticals of interest broadened the client's perspective, offering insights into vulnerabilities and exploits on common technology and infrastructure, in addition to emerging threats that may impact the sectors in times to come.

This cross-sectoral approach not only enhanced the client's understanding of potential risks but also facilitated the development of more comprehensive and adaptable security measures, which accounted for future cyber risks as well.

The culmination of these efforts provided targeted intelligence, enabling informed strategic decisions, and ensuring proactive measures to safeguard critical systems and data against evolving threats in the transportation sector.