Gemserv
A Talan Company

As an award-winning cybersecurity provider, Gemserv created a bespoke cyber threat intelligence monitoring and reporting solution for a global manufacturer.

THE CHALLENGE

The client is a global multinational manufacturer of power and propulsion systems. This organisation produces integrated systems that are used in multiple sectors including defence and transport in the United States. The client required a solution that ensured the security posture of their products. Both physical and nonphysical assets were potentially vulnerable to an ever-evolving landscape of cyber threats.

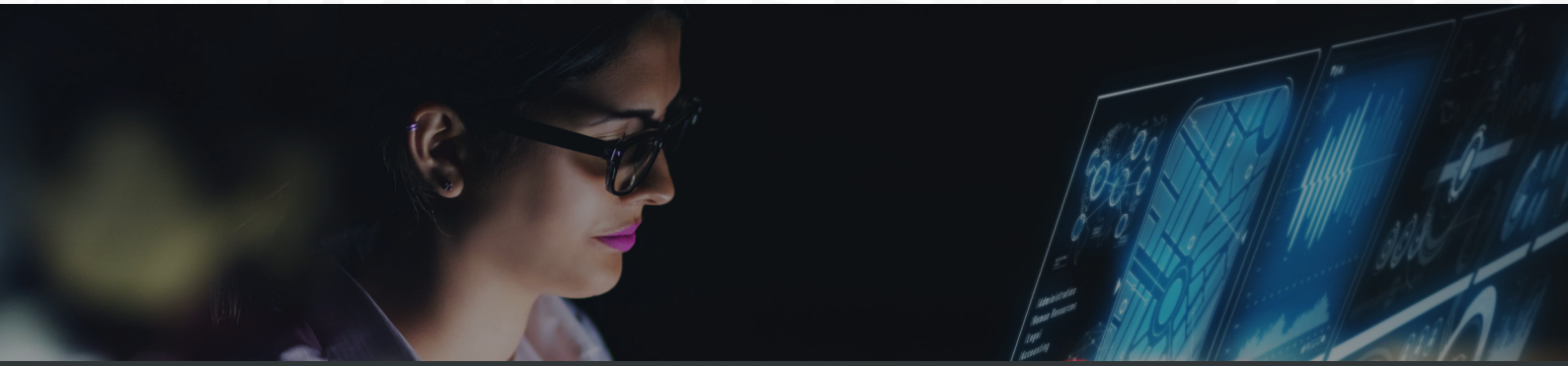
Product cyber security is the ability to resist and remain resilient to threats throughout the full product lifecycle. It involves deterring, defending against, recovering from, and adapting to malicious acts designed to compromise products.

The client's aim was to safeguard themselves against intentional damage, weaponization and exploitation.

In addition, they looked to protect the integrity, confidentiality, and availability of their system(s) and data. To better manage this posture, the client needed up-to-date and relevant product cyber security threat intelligence.

The client articulated they had three primary use cases that needed coverage; these were:

- Monitoring of past or emerging threats and attacks to cyber physical systems across a diverse set of verticals.
- Monitoring of past or emerging threats and attacks to cyber physical systems affecting suppliers and competitors.
- Monitoring changes to regulatory requirements that could lead to attacks from Nation States or other threat actors.



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 product cybersecurity intelligence plan for the client. Our initiative ensured the resilience and integrity of the client's cyber-physical systems, fortifying them against a wide range of threats. To achieve this, we also ensured that they met regulatory requirements across different verticals.

Furthermore, Gemserv delivered bespoke weekly reports covering up-to-date and relevant product-specific cyber security threat intelligence. We supported the client with regular consumption of actionable threat intelligence feeds, leading to more effective cyber defensive practices, enhanced cyber security strategies, and more targeted mitigation measures.
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/Region Specific Activity
- MITRE Attack Framework Analysis
- Technology Stack Monitoring
- Profiling of Advanced Persistent Threats
- Brand Intelligence
- Supply Chain and Competitor Intelligence
- Geopolitical Intelligence

THE IMPACT

The resulting benefits for each required use case were, respectively:

Accounting for attacks and/or exploits affecting suppliers and competitors, and that products remained secure following implementation. It is important to remember that threat actors are bound to repeat successful attacks, hence the need to ensure ongoing monitoring remained in place.

Identifying and investigating Tactics, Techniques, and Procedures (TTPs) used for cyber-attacks within sectors of operations (or adjacent sectors). We considered effective mitigations within the client's operational environment.

Monitoring changes in the political, regulatory, legal, and environmental domains and any retaliation-type activity could be averted.

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

Contact Us:
BD@gemserv.com