Blueliv.

MSSP CASE STUDY
LATAM Consultancy

Big 4 consultancy adopts Blueliv to serve increasing customer demand for threat intelligence services

Location	Latin America region
Number of employees	5,000
Sector	'Big 4' consultancy offering cybersecurity services to major enterprise customers in the financial services sector

CHALLENGES

- Detect and respond to threats in the fastest way possible - including within the deep/dark web - to protect clients in real time before risks become reality
- Allay customer fears about domain and brand reputation with the ability to identify incidents early and mitigate their impact
- Grow the business - Achieve rapid and seamless adoption and time to revenue
- Innovate at scale without prohibitive cost overheads
- Differentiate the market offering and provide Cyber leadership in the local market

SOLUTION

Threat Compass

Blueliv's multitenant, modular cyberthreat intelligence platform.

RESULTS

- Rapid ROI from modular pay-as-you-use cost base
- High customer uptake, engagement and satisfaction
- Significantly improved service quality and value with no infrastructure investment
- Easy integration and management thanks to automated APIs
- Enhanced customer protection against a multitude of advanced threats
- Solid foundation for future service innovation and customer acquisition

> “ **Using the Blueliv solution has increased our service quality, bringing more results to our customers, and all without the need for internal infrastructure. Blueliv accelerates our capability to provide customers with Threat Intelligence services. With in-house resources alone, it would have taken years to achieve the same.** ”

Cybersecurity Leader

OVERVIEW

This organization is a major national subsidiary of one of the 'Big 4' global consultancies, situated within the Latin America region. It employs around 5,000 staff and works with leading enterprise customers, delivering a range of services to optimize business success. This includes the provision of managed cybersecurity services, which the organization was looking to enrich via a better approach to threat intelligence. The goal was to provide a highly effective solution that could match its needs and help it reinforce differentiation in the market.

CHALLENGES

This consultancy's brand has a worldwide reputation for service innovation and saw the increasing enterprise demand for managed security services as an opportunity to meet customer needs and cultivate market leadership.

In particular, the consultancy was facing repeated requests for additional measures to assure brand protection and domain protection by enterprise customers concerned by the escalating volume, complexity and pervasiveness of cyber threats – particularly from within the deep/dark web.

As existing SOC service providers, the consultancy had witnessed first-hand how monitoring of customers' internal environments could not be considered comprehensive without the support of Threat Intelligence (TI) to proactively identify potential threats, and quickly identify live incidents (such as a leaks of data, fake domains, leaked credentials, etc.). For this reason, the consultancy was keen to proceed with a new TI partner possessing the requisite capabilities to help build enhanced managed security services.

Its prior experience of working with TI partners had not delivered the anticipated results, largely because of those partners' failure to understand the local enterprise market, and also – critically – because of a lack of modularity that would enable the consultancy to extract optimum value from specific areas of TI coverage instead of paying for a comprehensive suite that would never be fully utilized.

As well as complete modularity of offering, breadth of threat intelligence sources and a solid understanding of local market dynamics, the consultancy also sought a TI provider with advanced API integration in order to maximize ease of adoption and automation with internal processes.

SOLUTION

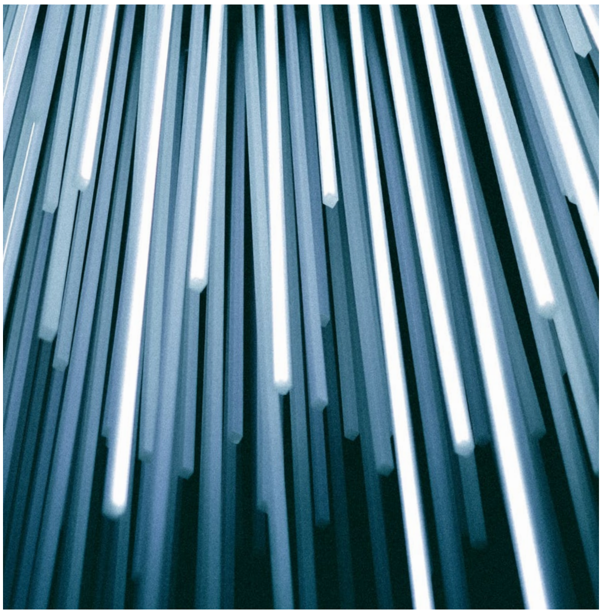
The consultancy became aware of Blueliv by researching the market and encountering its focused MSSP-oriented approach to delivering threat intelligence capabilities, working with the likes of Telefonica and many others. Blueliv's well-established understanding of national and regional market dynamics in Latin America were also appealing and reassuring.

The consultancy was also attracted by Blueliv's adaptive, modular technology: Threat Compass. Following a very successful proof of concept exercise (20 days in total), the consultancy was able to rapidly onboard key modules from this multi-tenanted, subscription-based platform to cover an initial cohort of 7–8 major enterprise customers, mostly in the financial services sector. This leveraged Threat Compass's automated API integration to plug-in seamlessly with the consultancy's internal processes and complementary services concerned with monitoring internal environments.

The core modules adopted from Blueliv are Credentials, Data Leakage, Credit Cards and Dark Web; each providing structured, actionable intelligence collected and abstracted from open, closed and private data sources in real-time via a combination of machine automation and highly skilled analysis by human cyber threat researchers.

> **“ Modularisation was the main differentiator; we only want to pay for what is used. We had great results from the proof of concept, and we saw the Blueliv team as a strong potential partner. ”**

Cybersecurity Leader



RESULTS

The initial set up was very fast, enabling rapid time to revenue. With Blueliv's support, the consultancy could accomplish service setup for a major financial services client in less than 1 week; in some cases, just 3 days.

Managed services overall have also improved since the implementation of Blueliv. Regular notifications about malware and other campaigns help the consultancy better understand the threat landscape in general. The 'news' information provided is greatly valued and readily shared with customers. Today, customers realize that TI brings them far greater insights than simply brand protection. Now, customers are equipped to look out for the threat actors, and try to analyze the broader

> **“ When we put Blueliv into production, we saw lots of results about compromised credentials and the clients were surprised with the volume and had no idea they'd been exposed. Some of the most revealing data leakage instances have been around GitHub and GitLab detection. The clients saw sensitive information that they had no idea was published, including internal projects with passwords. This helped us really open their eyes. ”**

Cybersecurity Leader

landscape that applies to their specific organization – Blueliv provides the ability to stay ahead of news rather than following it.

It is still comparatively early to determine ROI, but the use of modular, pay-as-you-use technology coupled with automated API integration has provided solid foundations for a low-opex, high-yield services platform. The consultancy is also bullish about its ability to bring its TI-enriched managed security services to many more enterprise customers, increasing revenue and market share.

NEXT STEPS

The consultancy and Blueliv have developed a positive partnership that is well set to deliver further results in the future.

Among the near-term objectives is customer acquisition, with the consultancy stating it expects to increase the volume of customers served by its services using Blueliv.

Fueling this will be further service innovation - potentially using additional modules from Threat Compass – so that more customer requirements can be met from an even greater scope of overall TI capabilities.

BECOME A BUSINESS PARTNER

Grow your business, increase sales and enhance your threat intelligence capabilities.

blueliv.com/partners

twitter.com/blueliv

linkedin.com/company/blueliv

info@blueliv.com

For more information, visit **www.blueliv.com**