MERCANTIL ANDINA SUCCESS CASE

INSURER REDUCES NOISE AND OPERATES CYBERSECURITY PROFICIENTLY

Mercantil Andina

Mercantil Andina is one of Argentina's top insurance firms. As a 100-year old company with nearly 800 employees that provides insurance products to more than a million policyholders, they are committed to not just operating cybersecurity for the benefit of all their stakeholders, but also doing so efficiently.

SUMMARY

Mercantil Andina needed to improve the working lives and efficiency of their security operations team. By using Lumu to operate cybersecurity more proficiently, they have gained unified visibility and an overall more robust, resilient cybersecurity operation.

THE PROBLEM: UNIFY COMPROMISE VISIBILITY

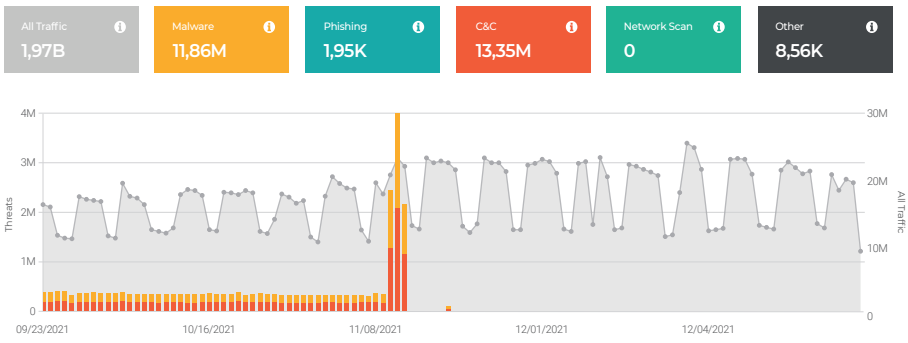
Mercantil Andina's cybersecurity operations team was overwhelmed by an incredible amount of alarms, of which many were false positives. Despite having a large cybersecurity stack with many tools at their disposal, distinguishing between real internal compromises and pure noise was proving to be time-consuming.

Investigating potential incidents required collecting information from disparate sources, which only compounded the difficulty of addressing alerts. "We had the problem of not knowing what was the real, original source of contacts with the adversary," said Mercantil Andina CISO, Daniel Manrique. This lack of unified visibility was causing the operation of the cybersecurity infrastructure to be difficult and leading to the security operations team feeling burnt out.

Their cybersecurity leadership recognized the critical need to operate cybersecurity more efficiently.

THE SOLUTION: OPERATE CYBERSECURITY WITH LUMU

Lumu Insights provides the unified visibility needed for the scope of the challenge facing Mercantil Andina's security operations team. Lumu Insights collects, standardizes, and analyzes network metadata from various sources in real time. Anomalous activity is passed through a "deep correlation" step, ensuring that the false positive rate is kept to a minimum.



Lumu is built to simplify the life of the security operator. Related contacts are grouped into a single incident, rather than thousands of alerts. The Lumu portal provides a unified view of all activity related to the incident, right down to the individual assets talking to the adversary.

Additionally, when operators need to investigate incidents, they can find all the information they need, right in one central location. Right from the portal, they can track the frequency of contacts and how the compromise is spreading to individual assets or shifting to different methods of attack. Contextual information like relevant MITRE ATT&CK Matrix™ techniques, playbooks, and 3rd party articles and resources are also available to help operators get the necessary background information for each incident.

HOW LUMU HELPED

The team noted how easy it was for Lumu to start collecting data and how quickly it was able to start generating value.

Thanks to Lumu's unified visibility, the contextual information provided, and the fact that individual assets in contact could be identified, they were able to operate cybersecurity more efficiently. In consequence, they were no longer overwhelmed by false alerts.

By starting to measure compromise with Lumu, their overall cybersecurity posture has improved. Now they are able to track which tools are performing suboptimally and which ones are only producing noise.

"What I like about **Lumu** is that it's an agnostic product. All industries have similar cybersecurity challenges around having unified visibility of the compromises already existing in their networks. There was nothing about our particular industry that made it more difficult to deploy Lumu. Because of the way that **Lumu** is conceived, it provides value to any company in any industry."

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io