



## TOPITOP CASE STUDY

# RETAILER ENHANCES EFFICIENCY IN THREAT DETECTION AND RESPONSE

Topitop was founded in 1983 and is one of the top-ranking Peruvian textile manufacturer-exporters.



## SUMMARY

Boasting a modern industrial complex with five textile plants equipped with the latest machinery, hundreds of employees, and an export operation to more than 5 countries, Topitop required a solution that would allow them to strengthen their network security while increasing efficiency in their cybersecurity operation.

## WHAT THEY NEEDED

Topitop's operation cannot be interrupted, that's why they were looking for a quick and easy-to-deploy solution that would enable them to get visibility into compromise across OT and corporate devices connected to the network, while reducing mean time to detect (MTTD), and automating time-consuming response tasks.

## THE SOLUTION

Eradicating blindspots in such a large network requires modern cybersecurity practices. Bearing that in mind, Topitop decided to implement Lumu Defender, which enabled them to:

- **Identify anomalous activity on critical network segments:** Lumu quickly adapted its threat intelligence engine to Topitop's large network. This helped them uncover existing communication to adversarial infrastructure.
- **Get real-time visibility and correlation of compromises:** Lumu's illumination process simplified the orchestration of existent threat intel sources, and provided Topitop with confirmed compromise and actionable intelligence to understand who, when, and how their organization was being targeted.
- **Automate threat detection and response:** Lumu's frictionless integration capabilities allowed Topitop to anticipate incidents and automatically eradicate threats with precision.
- **Prioritize efforts and focus on urgent actions:** Lumu's network labeling capabilities gave Topitop accurate insights into which network segments required immediate attention.

## BENEFITS OF LUMU

**Quick time to value:** Lumu being a SaaS solution gave Topitop complete asset-level visibility quickly after the activation of their subscription.

**Align the cybersecurity stack on the same page:** Integration and orchestration capabilities allowed Topitop to get the most out of their cybersecurity investments.

**Increase protection of critical assets:** Topitop was able to anticipate threats on their most critical network segments and assets with speed and precision.

**Accuracy in compromise eradication:** Asset-level visibility provided allowed Topitop to pinpoint contacts with adversarial infrastructure and perform eradication tasks effectively.

*"Lumu allows us to measure compromise in real time, identifying threats across the network and removing them at speed."*

CONTACT LUMU  
SALES@LUMU.IO

[www.lumu.io](http://www.lumu.io)

