



**CASE STUDY:**

40% cost savings  
for logistics leader  
with a threat-led  
transformation

**INDUSTRY: LOGISTICS**

## About the Client

The client is one of the world's largest transportation and logistics providers, with a workforce of more than 70,000 employees and subsidiaries in over 100 countries. The company plays a vital role in global supply chains, managing shipping, cargo, and distribution networks that are essential to international commerce.

As a result, the organization faces heightened cyber risk from both state-sponsored adversaries and organized crime groups.

## Client Challenge

Recent years have shown that logistics providers are frequent targets of ransomware attacks and supply chain compromise, due to their critical role in global trade and their reliance on interconnected IT and OT systems. This elevated threat landscape made it essential for the client to strengthen resilience and reduce operational exposures.

The client's existing service operations relied almost exclusively on manual tasks and processes to perform monitoring and response. This dependence on human effort created delays, inefficiencies, and increased the likelihood of missed detections.

In addition, the incumbent provider offered limited transparency, operating as a "black box" with little contextualization of alerts. This left the client without the visibility or collaboration needed to effectively prioritize and mitigate risks.

The client sought a managed security services partner capable of supporting all aspects of their operations, including 24x7 Level 1 SOC coverage. Their objectives included automating routine activities, reducing time to detect and respond to incidents, and improving SOC effectiveness with measurable KPIs, while leveraging their existing tools and investments.

## Benefits



**Reduced costs:** Over 40% savings through automation and streamlined SOC operations



**Less exposure:** Automated 80% of Level 1 triage, reducing attack windows, and improved security visibility.



**Maximized investments:** Integrated existing SOAR and SIEM tools for greater efficiency



**Stronger resilience:** Threat-led use case management aligned to ransomware and supply chain risks, and better transparency and collaboration through the CyberProof's service delivery platform



CyberProof helped us dramatically improve our Mean Time to Respond (MTTR), reducing exposure windows and minimizing business impact. Within weeks, we gained clearer visibility, greater automation, and stronger defenses than we ever had with our previous provider.”

— Head of Cyber Defense

# Our Solution

CyberProof was selected to provide a fully managed security monitoring capability focused on addressing the client’s most pressing threats and operational exposures. Partnering with Microsoft, CyberProof implemented a scalable SOC model that combined automation, threat-led detection engineering, and collaborative transparency.

Key solution components included:

**24/7 monitoring and enrichment:** Continuous global coverage reduced detection times and improved MTTR, ensuring exposures were identified and contained quickly.

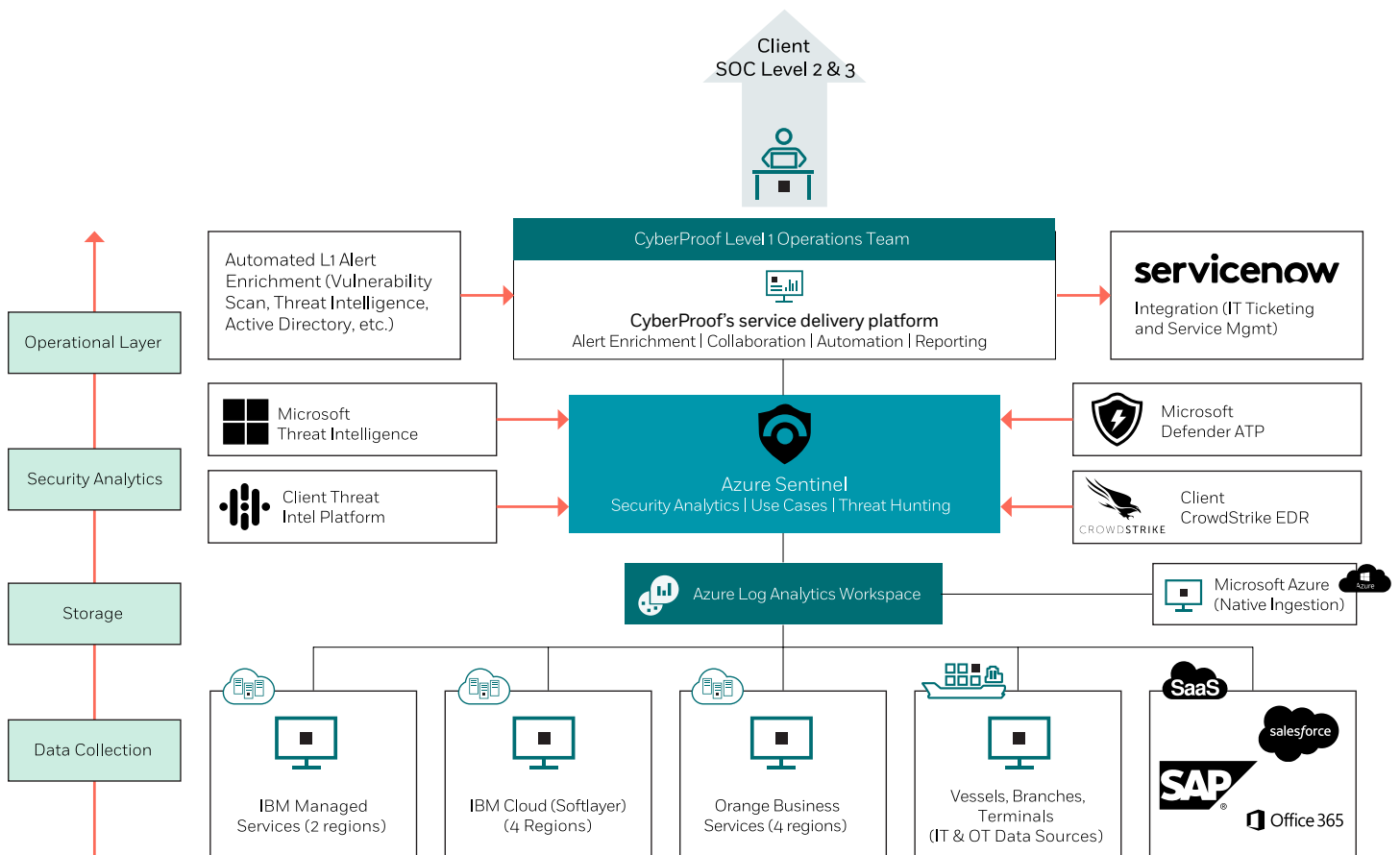
**Use Case Management and Catalog:** Customized detection rules, prevention controls, and digital playbooks aligned with MITRE ATT&CK TTPs relevant to the logistics sector. This enabled automation of up to 80% of Level 1 activities, including alert triage, investigation, and response.

**Integration with existing technology:** CyberProof built custom integrations with the client’s SOAR and SIEM tools, extending automation and orchestration while preserving prior technology investments.

**Collaborative operations through the CyberProof Defense Center (CDC):** With built-in ChatOps, the CDC provided a single view of SOC workflows, increasing transparency and enabling co-sourced operations between the client’s team and CyberProof analysts.

**Scalable, cloud-native architecture:** The Microsoft Azure Sentinel–based environment offered flexibility to expand into OT and IoT monitoring as the client’s needs evolve.

This approach reduced operations costs by more than 40%, automated the majority of repetitive Level 1 tasks, and improved resilience against ransomware and supply chain attacks, all while enhancing visibility, transparency, and long-term scalability.



**SERVICE ARCHITECTURE**

## About CyberProof

CyberProof, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security delivers industry-leading services to drive real business results. We believe that working closely with our customers and partners through a 'better security, together' services model jointly empowers us to defend against the greatest of threats. See: [www.cyberproof.com](http://www.cyberproof.com).

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum