

CASE STUDY:

Managed security services
for a large international
logistics company

INDUSTRY: LOGISTICS

Client background

A well-established, multinational transportation and logistics company approached CyberProof for assistance with security operations. The company is one of the largest operators internationally, with subsidiaries and offices in over 100 countries around the globe and more than 70,000 employees.

Client challenge

The customer's existing service operations relied almost exclusively on manual tasks and processes to perform monitoring and response security operations.

The client was interested in eliminating as many of these manual processes as possible without compromising on accuracy and replacing them with more efficient, automated operational processes.

They were looking for a Managed Security Services Provider (MSSP) that offered a transparent and collaborative approach, replacing the "black box" solution of the incumbent provider. They were also looking for a vendor that would augment the capabilities of their existing security operations center (SOC) and security team.

The goal

The client sought to engage with an MSSP who could support all aspects of their security operations – including 24x7 coverage for their Level 1 SOC activities.

They were interested in introducing more efficient, automated processes; at the same time, they also needed to continue leveraging their existing tools and technologies. They wanted to reduce the time to detect and respond to incidents and improve the effectiveness of their operations based on clearly measurable KPIs.

Benefits



Improved security visibility by expanding the organization's monitoring in cloud environments, using Azure Sentinel SIEM.



Greater operational efficiency by automating 70-80% of Level 1 alert notification, triage, investigation and response activities.



Reduction in operations costs of over 40%, achieved by integrating CyberProof's cloud-native tools and automations.



Better transparency and collaboration with full visibility into SOC operations.



CyberProof's solution provided the client with dramatically improved Mean Time to Respond (MTTR), thereby reducing the level of risk and minimizing impact. CyberProof's virtual analyst, SeeMo, contributed to their ability to reduce human efforts and cut costs.

- **Head of Cyber Defense**

Our solution

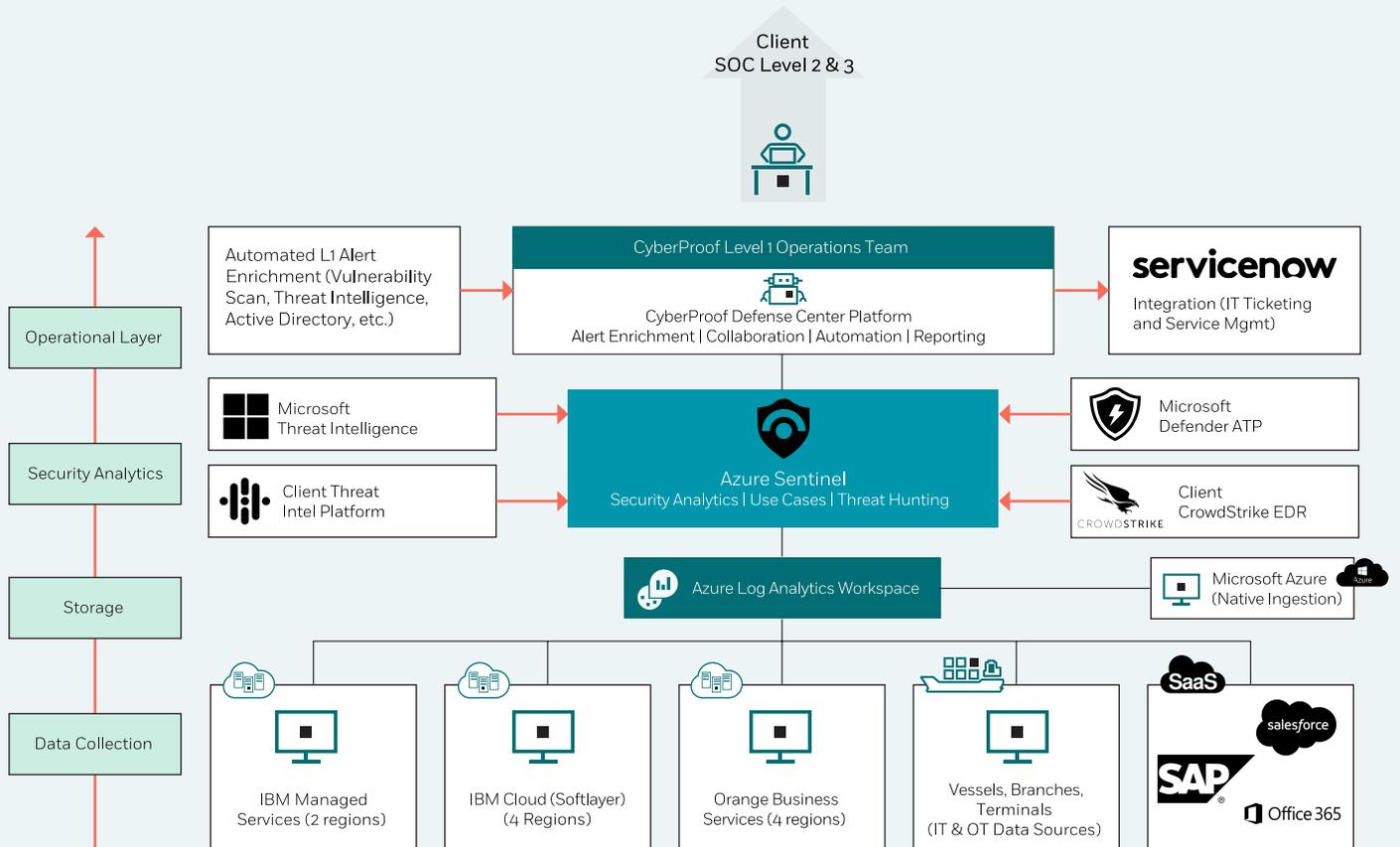
CyberProof was selected to provide the client with a fully managed security event monitoring capability. Working together with Microsoft, one of our strategic partners, CyberProof developed a security analytics and SOC monitoring proposition that has the ability to scale up, as well as down – providing the client with the level of flexibility they required in adopting new technologies and services.

CyberProof deployed a full range of managed cybersecurity services, including:

- 24/7 event monitoring, event enrichment, and triage
- Incident response with customized threat detection rules, use cases, and digital playbooks
- Use Case Management that is fully integrated with the CyberProof Defense Center (CDC) platform- our next-generation service delivery platform that leverages automation, orchestration and collaboration capabilities to deliver co-sourced SOC services.

CyberProof successfully automated up to 80% of the client’s L1 activities by leveraging our Use Case Catalog - a library of customized Use Case Kits consisting of prevention controls, detection rules and response playbooks.

SERVICES ARCHITECTURE



About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations. For more information, visit www.cyberproof.com.

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

cyberproof.com