CyberProof®
A UST Company

CASE STUDY:

Security services for a provider of travel technology solutions

INDUSTRY: TRAVEL

About the Client

The client chose CyberProof to provide advanced Managed Detection & Response (MDR) services including 24x7 L1 & L2 SOC services and platform management services – utilizing Microsoft Sentinel, Splunk, XSOAR, CrowdStrike and Cortex XDR security technologies. The client also uses CyberProof's Use Case Management Service to manage existing use cases and develop new ones.

The Problem

The client had a variety of challenges and sought a strategic cybersecurity partner to assist them in reaching their goals. They were looking to embrace Microsoft Security Suite and were making a major shift, porting their applications to the cloud. They needed a strong Microsoft Azure security services partner to help build a path towards a cloud-native security operation.

Operationally, they wanted to move away from the black-box security service provided by their incumbent vendor and were interested in a hybrid, transparent and flexible delivery model. They were looking for a partner that would be able to implement significant change while they continued to retain control.

The Solution

In the first phase of this project, CyberProof assisted the client in setting up Microsoft Sentinel SIEM and building a cloud data lake. All native and non-native data sources were connected to Sentinel SIEM, and the required detection rules and playbooks were created. In the second phase of the project, CyberProof took over the 24x7 security operation service - L1 and L2 services leveraging Microsoft Sentinel, Splunk, CrowdStrike and Cortex XDR technologies.

We also supported the client with the setup and management of the Cortex XSOAR platform and helped to focus their threat detection efforts by using our Use Case Factory (UCF) to manage their existing use cases while continuously creating, testing and deploying new ones as their threat landscape changed.

Benefits

Designed and implemented a cloud-native security threat monitoring solution using Microsoft Sentinel

Extended security monitoring to new cloud sources and services

Established sustainable Use Case Management and Governance program

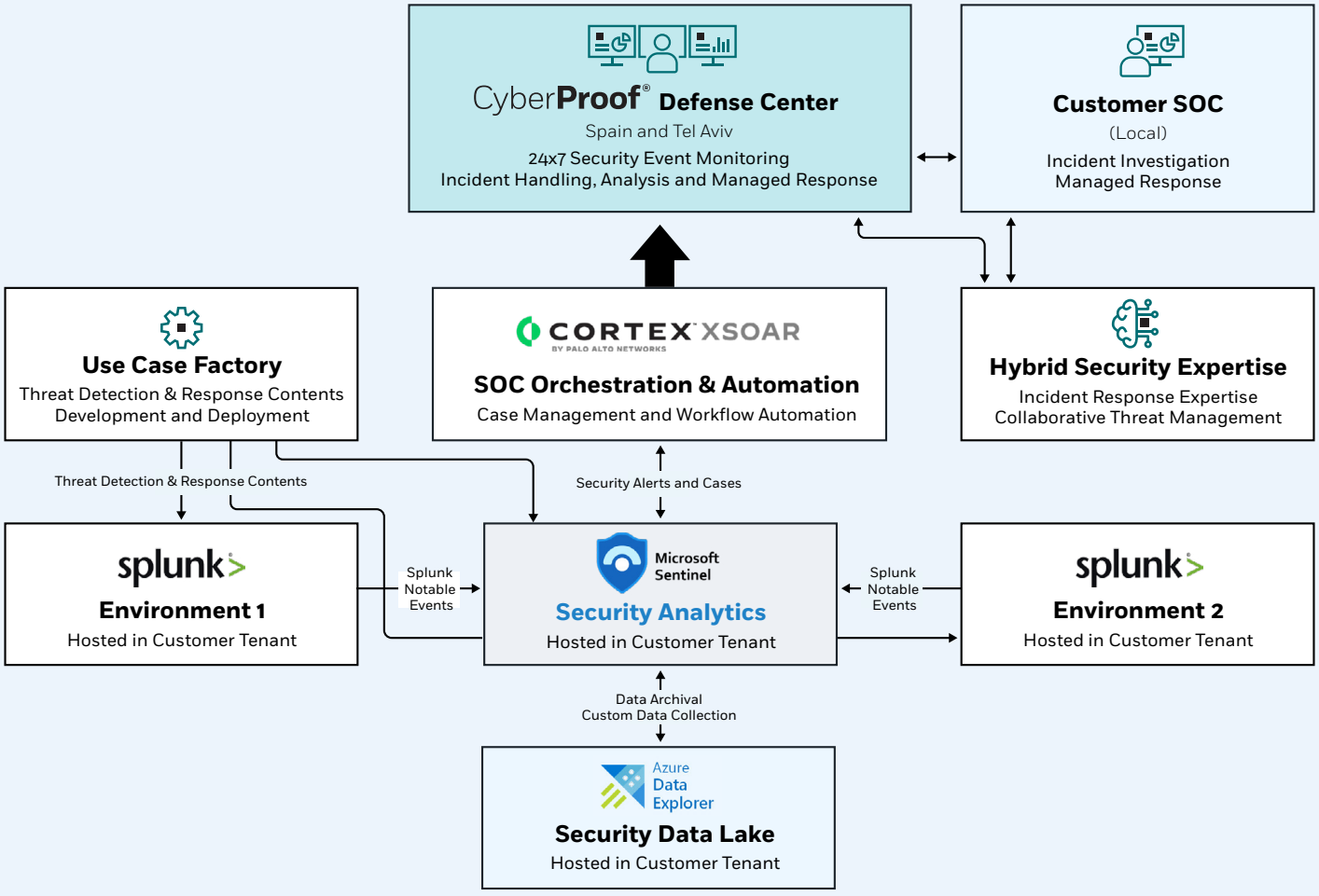
Provided access to highly skilled certified Microsoft Security professionals

Developed seamless processes for migrating to cloud-native SIEM from legacy technology

Maintained control while leveraging CyberProof resources in a flexible and agile manner

The scope for this engagement was:

- A starting ingestion volume of 9TB/day data ingestion
- Over 60,000 endpoints
- Hybrid engagement model, with dedicated experts for L2 and Use Case Factory teams - managed by a Service Delivery Manager
- Managing all security tools – Sentinel SIEM, Splunk SIEM, Palo Alto XSOAR & XDR, Azure Data Lake, Splunk Data Lake, etc.
- The technology stack included: Sentinel & Splunk SIEM, Palo Alto XSOAR & XDR, CrowdStrike



SERVICE 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