

**CASE STUDY:**

Reducing exposure  
and improving MTTR  
for a global provider  
of travel and leisure  
software services with  
24x7 MDR

**INDUSTRY: TRAVEL**

## About the Client

The client is a leading provider of travel and leisure software solutions that supports airlines, hotels, and agencies worldwide. Operating at global scale with millions of daily transactions, the organization required advanced cybersecurity capabilities to safeguard sensitive customer and partner data.

To strengthen defenses, the client was looking for Managed Detection & Response (MDR) services, including 24x7 L1 and L2 SOC operations, platform management, and continuous Use Case Management. By leveraging technologies such as Microsoft Sentinel, Splunk, XSOAR, CrowdStrike, and Cortex XDR, the client sought to modernize its SOC with a cloud-native model while maintaining flexibility and transparency.

## The Problem

As the client undertook a major cloud transformation, migrating applications and services to Microsoft Azure, their reliance on a fragmented set of tools and an opaque “black box” security provider left them exposed. They lacked clear visibility into threats across their hybrid environment, which increased risk at a time when adversaries frequently target the travel sector with fraud, ransomware, and data theft campaigns.

Operationally, the client required a more transparent and collaborative model — one that would enable them to retain control of decision-making while benefiting from specialized expertise. They also needed to integrate and optimize a broad technology stack, including Microsoft Sentinel, Splunk, XSOAR, CrowdStrike, and Cortex XDR, without creating new blind spots.

Finally, the client recognized that without a sustainable Use Case Management and Governance program, detection engineering would lag behind the evolving threat landscape. To reduce exposure and strengthen resilience, they sought a strategic partner to deliver 24x7 MDR services, automate routine activities, and establish a path to a fully cloud-native SOC.

## Benefits



### Extended visibility:

CyberProof ingested over 9TB/day of data across 60,000 endpoints, providing comprehensive monitoring of hybrid and cloud environments.



### Faster response:

With 24x7 MDR operations, CyberProof reduced exposure windows and improved Mean Time to Respond (MTTR) against ransomware and fraud attempts.



### Sustainable detection:

Through the Use Case Management service, CyberProof ensured detection rules and playbooks continuously evolved with the threat landscape.



### Cloud-native resilience:

CyberProof delivered a seamless migration from legacy SIEM to Microsoft Sentinel, extending monitoring to new cloud sources while maintaining compliance and control.



CyberProof gave us the visibility and expertise we needed to modernize our SOC. By ingesting massive volumes of data across our hybrid environment and continuously updating use cases, they helped us reduce exposure and improve response times. We now have greater confidence in our ability to defend against evolving threats while maintaining full control of our operations.”

— VP of Security, Global Travel Technology Provider

# The Solution

CyberProof partnered with the client to design and operate a fully managed, cloud-native SOC aligned to the organization's evolving threat landscape and cloud transformation strategy.

Key solution components included:



**Cloud-native SOC build:** Deployment of Microsoft Sentinel SIEM and a cloud data lake, integrating all native and non-native sources. The initial volume included 9TB/day ingestion across 60,000 endpoints, ensuring comprehensive visibility.



**Use Case Management (UCM):** Ongoing management of use cases, with continuous development, testing, and deployment of new threat scenarios as the landscape evolved. This ensured detections remained relevant and prioritized against exposures most critical to the travel sector.



**Threat-led detection and response:** Creation of customized detection rules and playbooks mapped to adversary TTPs. Integration of Microsoft Sentinel, Splunk, Cortex XDR, CrowdStrike, and XSOAR allowed for coordinated detection and automated response.



**Governance and transparency:** Full visibility into SOC operations through the CyberProof Defense Center, enabling collaborative decision-making while maintaining client control.



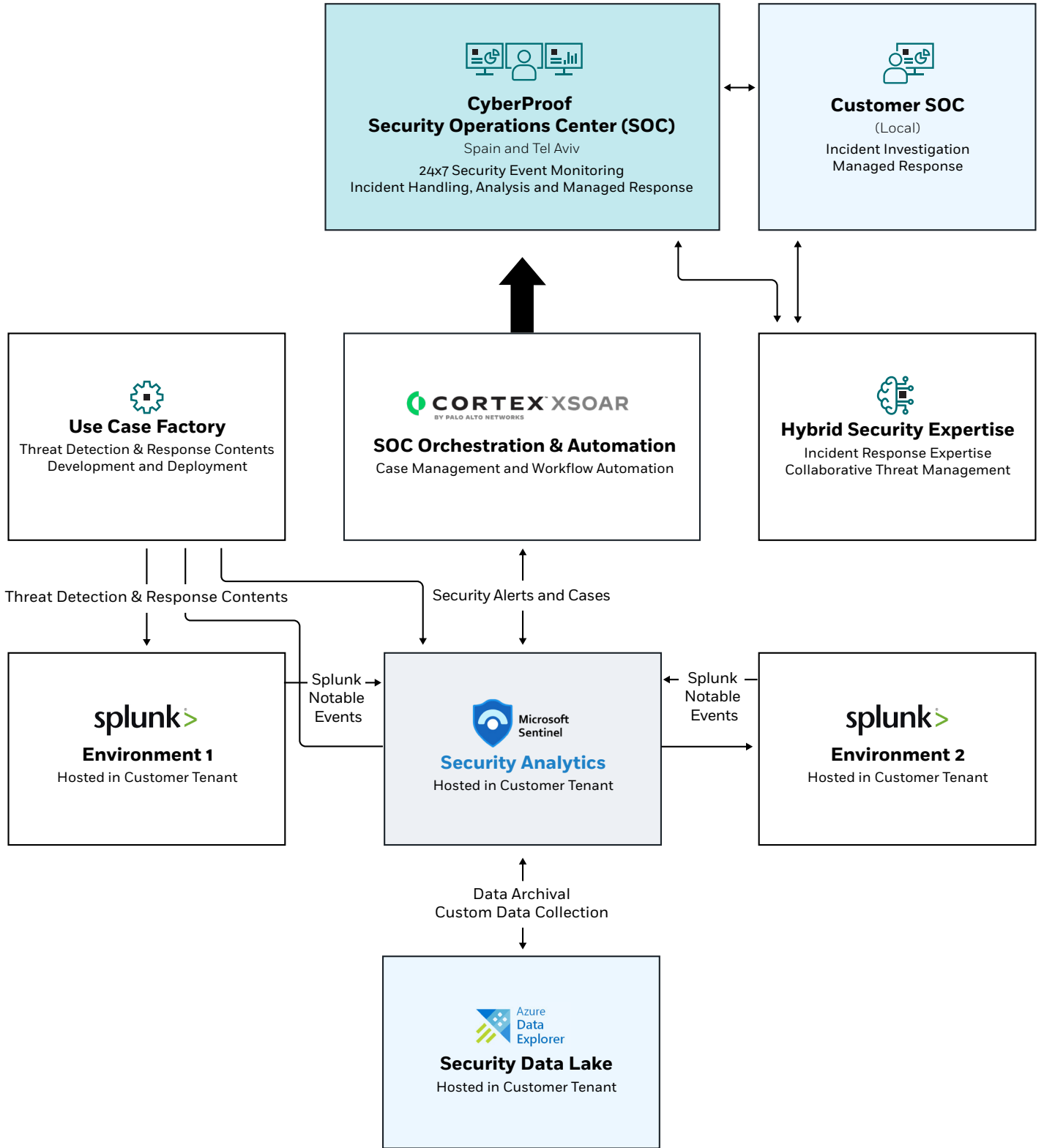
**24x7 MDR operations:** CyberProof assumed responsibility for L1 and L2 SOC services with a hybrid model, combining dedicated on-site expertise with remote delivery from CyberProof's global team.



**Technology optimization:** Supported the setup and management of the Cortex XSOAR platform and built seamless integrations to maximize the value of the client's existing security investments.

By combining cloud-native scale, 24x7 operations, and continuous threat-led use case management, CyberProof enabled the client to modernize its SOC, reduce exposure, and improve resilience against ransomware, fraud, and other threats targeting the travel sector.





**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