

CASE STUDY:

Threat-led security
transformation for a
multinational energy
company

INDUSTRY: ENERGY

Client background

The client is a multinational energy company engaged in producing natural gas liquids and petrochemicals. The company has operations in multiple locations around the world.

Client challenge

High-profile incidents, including the ransomware attack on Colonial Pipeline and the escalation of the Russia-Ukraine conflict, underscored the heightened risk to energy providers from both state-sponsored groups and cybercriminals. The client recognized that their existing security architecture left them exposed to ransomware, supply chain compromise, and potential disruption of critical OT systems.

At the same time, attrition among in-house security staff created gaps in expertise, limiting the ability to continuously monitor, detect, and respond to targeted attacks. These exposures were compounded by reliance on legacy, on-premises technology that lacked the visibility and scalability needed to defend against modern adversaries.

The client sought a managed cybersecurity partner to help them shift to a threat-led, cloud-native security stack based on Microsoft Sentinel and Defender, supported by advanced Managed Extended Detection & Response (XDR) services. The goal was to build resilience by aligning defenses to the tactics, techniques, and procedures (TTPs) most relevant to the energy sector.

Benefits



Reduced ransomware and OT disruption risk through threat-led monitoring



Improved visibility of critical exposures across IT, OT, and cloud



Faster incident detection and containment with Managed XDR



Strengthened resilience by aligning defenses to adversary TTPs



Our solution

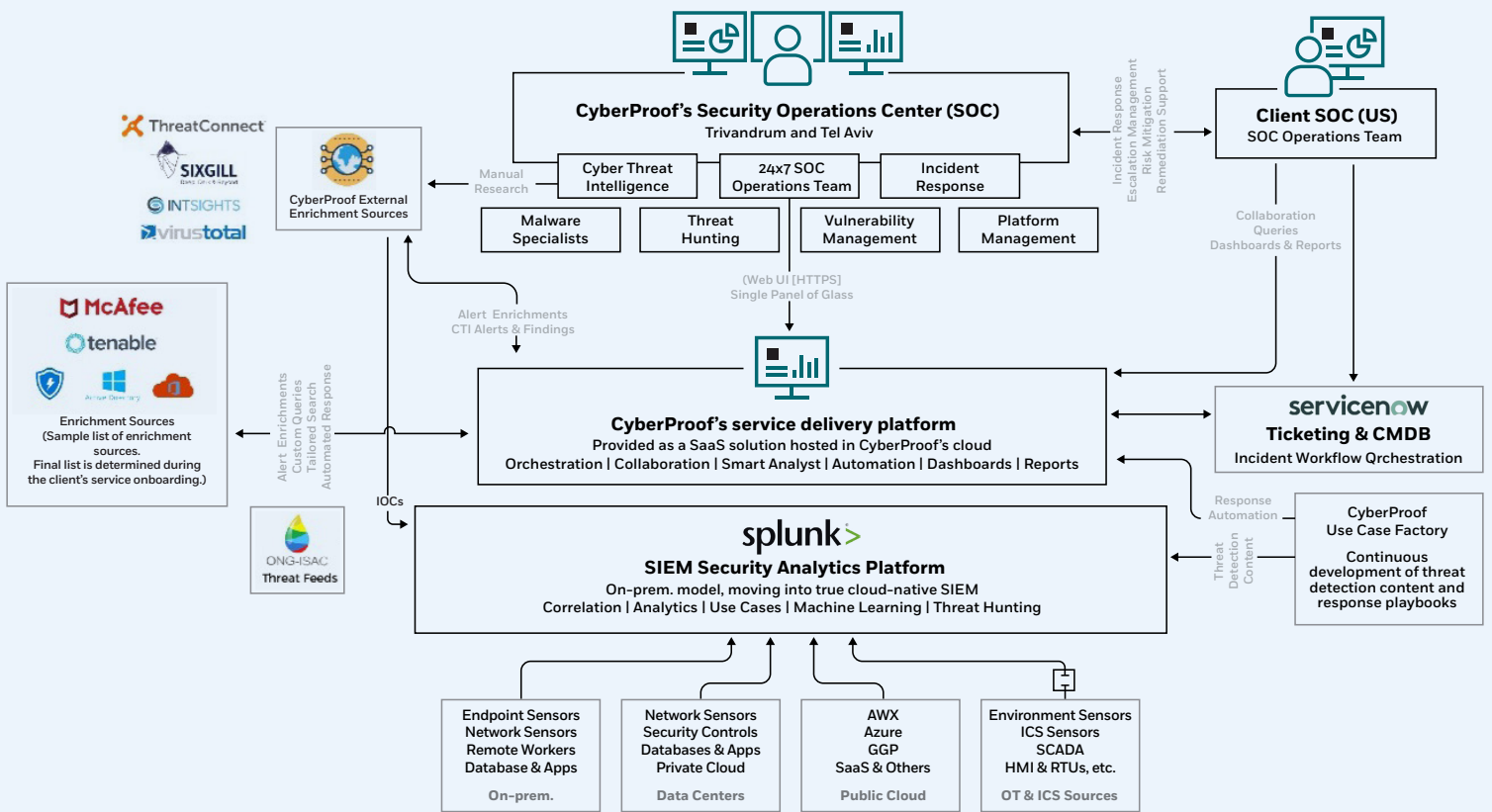
CyberProof’s team delivered an end-to-end security platform and service designed to address the client’s most critical threat exposures. Leveraging Microsoft Sentinel SIEM and Microsoft Defender, the solution replaced legacy on-premises systems with a modern, cloud-native security architecture.

The transformation program provided continuous visibility across both IT and OT environments, with monitoring aligned to adversary tactics and emerging threats facing the energy sector. Security operations

were mapped to the MITRE ATT&CK framework, ensuring detections and threat-hunting activities were structured around the techniques most frequently used by energy-focused adversaries.

CyberProof now manages and operates a complete set of next-generation security services, including Managed XDR, threat intelligence, threat hunting, managed EDR, and vulnerability management, ensuring defenses remain proactive, relevant, and resilient against evolving attacker techniques.

CYBERPROOF DEFENSE CENTER (CDC) PLATFORM ARCHITECTURE



By shifting from a technology-first to a threat-led security model, the client gained visibility into its most critical exposures, and aligned defenses with the adversaries most likely to target the energy sector. This

approach not only improved incident response times but also strengthened resilience against both state-sponsored and criminal cyber threats.

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.

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