



**CASE STUDY:**

# Proactive cyber defense for a complex hospitality network

**INDUSTRY: HOSPITALITY AND ENTERTAINMENT**

## About the client

The client, situated in the US, specializes in hospitality and entertainment services. It employs a significant workforce and maintains operations across several key states. The company's offerings include a wide range of entertainment and dining facilities, with an extensive network of gaming and tavern locations that are a high-visibility target for threat actors. These require continuous visibility and proactive management of its attack surface to minimize exposure and ensure business resilience.

## Client challenge

The client was looking to engage with a service provider adept in managing and operating their platform - one that could enhance the value delivered and ensure top-tier protection against cyber threats, and services that included thorough threat analysis and remediation.

The company already had a Security Incident and Event Management (SIEM) technology and an Endpoint Detection & Response (EDR) solution from a prominent vendor but required a partner that could maintain and enhance the technology's performance and extract its full potential in terms of cyber security.

The client aimed to:

- Efficiently manage and optimize existing cybersecurity solutions to reduce exposure and risk.
- Enhance cyber protection through proactive, threat-led detection and response.
- Develop and manage new use cases aligned to its most critical business and threat scenarios.

## Benefits



**Threat-led detection and response** CyberProof's analysts leverage advanced orchestration and automation to accelerate detection, containment, and remediation of high-priority threats.



**Continuous exposure management** Integrated visibility across diverse data sources reduces false positives, improves situational awareness, and strengthens control over the client's attack surface.



**Expert-driven threat intelligence** Nation-state-trained experts enrich operations with real-world insights from active threat environments, enhancing the client's defense against evolving adversaries.



**Operational efficiency and resilience** Cloud-native SecOps collaboration streamlines workflows across distributed teams, reducing time to respond while maintaining consistent, resilient operations.



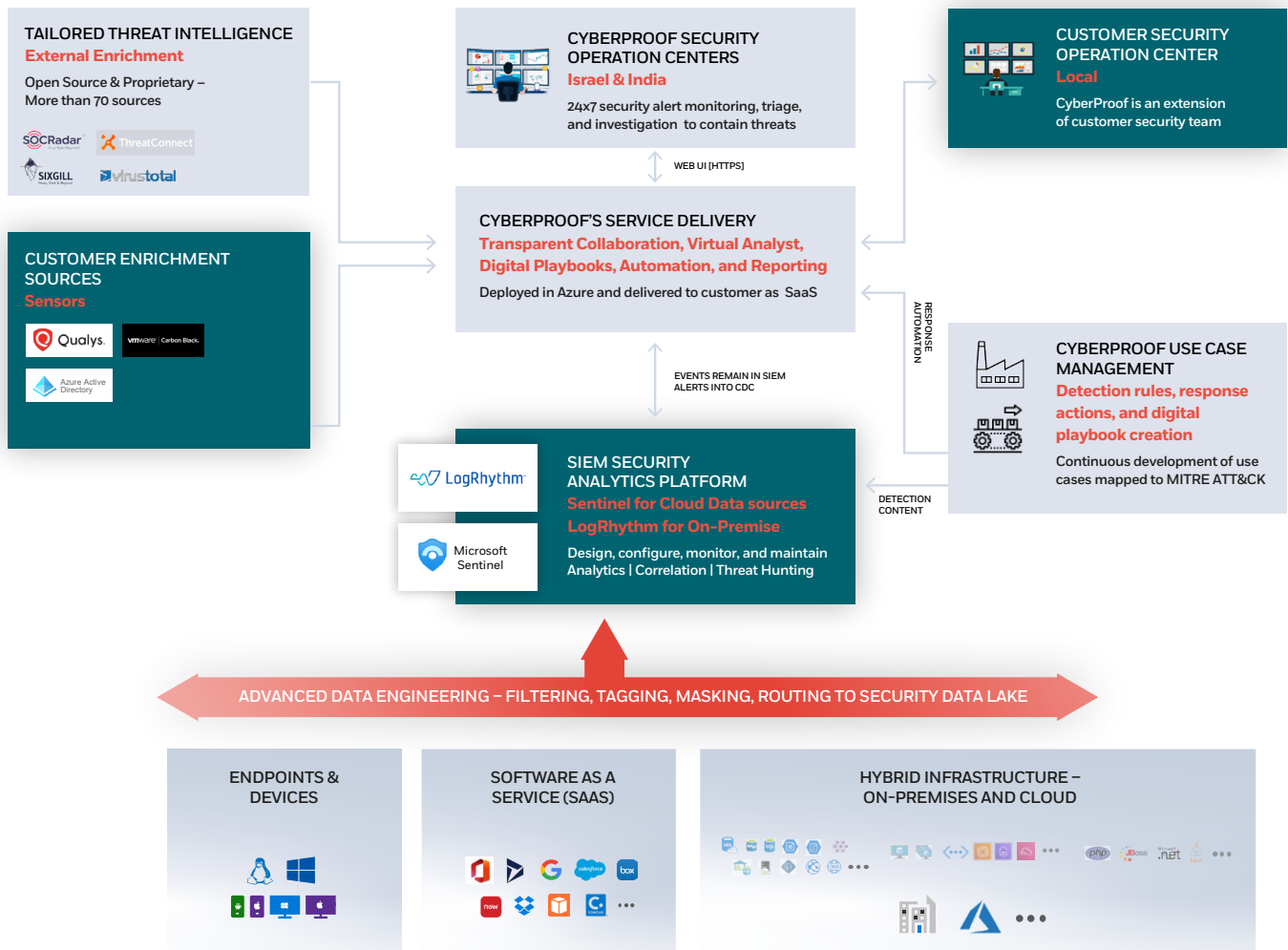
“Our partnership with CyberProof has sharpened our response to security threats. Their tailored enhancements to our security operations systems have led to a more efficient response process to minimize risks. The integration of CyberProof's Use Case Management service has provided greater focus and customization to mitigate industry-specific threats.”

Client Cybersecurity Director

# The solution

CyberProof partnered with the client to enhance and operationalize its existing SIEM and EDR investments, delivering full Managed Detection & Response (MDR) and Digital Forensics and Incident Response (DFIR) services. The engagement focused on strengthening threat visibility, optimizing detection content, and expanding the client’s capabilities into the cloud to enable a unified, threat-led defense model.

The CyberProof team implemented a tailored Use Case Management framework aligned to the MITRE ATT&CK® framework, designed to continuously identify and address the organization’s highest-risk threat scenarios. Over ten customized response playbooks were deployed to proactively contain threats, while advanced automation within the CyberProof service delivery platform reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).



## 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