# CyberProof®

A UST Company

**CASE STUDY:**

# Security Services for a Leading Hospitality and Entertainment Company

**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.

# The client's 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 was focused on:

- Efficient management of their existing cyber security solutions
- Enhanced cyber protection through proactive detection and response
- Development and management of new security use cases

# Benefits

- **High fidelity response** driven by cyber analysts and security tools that cut the time to response through orchestration & automation
- **Multi-team SecOps collaboration** with a cloud-native deployment that provides integration and orchestration, facilitating interaction between distributed teams
- **Nation-state expert enrichment** that brings real-world threat landscape experience from high-conflict cyberattack zones to SOC operations
- **Event data enrichment and insights** that provide additional context to facilitate faster, more effective prioritization of alerts
- **Fewer false positives** as data and logs are collected from multiple sources, reducing errors and time to detect
- **Established a rapid response process** to defend against advanced malware and ransomware threats
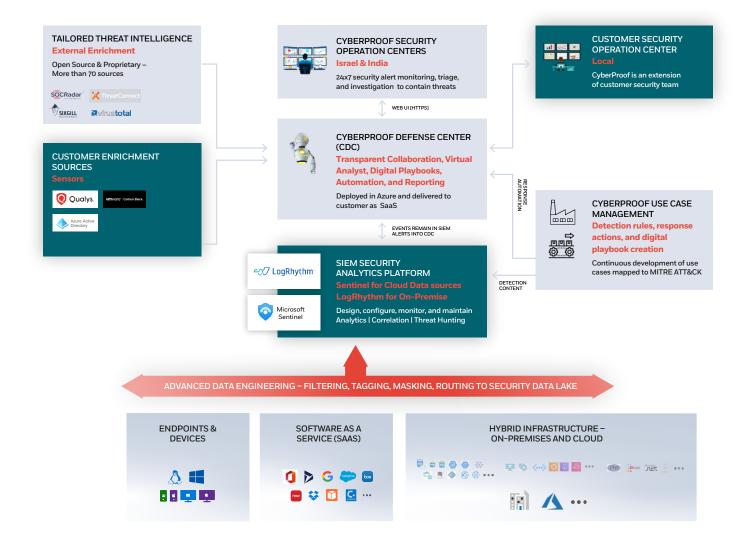
# A look at the numbers

- **Deployed over 10 tailored response playbooks** to proactively contain threats
- **Integrated services architecture** providing 360-degree coverage around cyber defense capabilities
- **Achieved over 50% of operational efficiency** by automating SOC procedures
- **Created 2 well defined, measurable KPIs** that drive service baselining and continuous improvement

"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

# Our solution

CyberProof partnered with the client to optimize their existing SIEM and EDR systems as well as provide them with full Managed Detection & Response (MDR) and Digital Forensics and Incident Response (DFIR) services. In addition, CyberProof's team expanded the client's systems into the cloud, taking an active role in the management of their current use cases and the development of new strategic ones through Use Case Management that met the needs of their Gaming Management System to identify specific anomalies. This initiative not only maintained the integrity of the client's pre-existing defense mechanisms but also augmented their overall security framework. As a result, the client now benefits from a robustly managed security operation, equipped with enhanced capabilities for the rapid detection and response to cyber threats.



**TAILORED THREAT INTELLIGENCE**
**External Enrichment**

Open Source & Proprietary – More than 70 sources

SOCRadar · ThreatConnect · SIXGILL · virustotal

**CUSTOMER ENRICHMENT SOURCES**
**Sensors**

Qualys · vmware Carbon Black · Azure Active Directory

**CYBERPROOF SECURITY OPERATION CENTERS**
**Israel & India**

24x7 security alert monitoring, triage, and investigation to contain threats

WEB UI [HTTPS]

**CYBERPROOF DEFENSE CENTER (CDC)**
**Transparent Collaboration, Virtual Analyst, Digital Playbooks, Automation, and Reporting**

Deployed in Azure and delivered to customer as SaaS

EVENTS REMAIN IN SIEM ALERTS INTO CDC

**CUSTOMER SECURITY OPERATION CENTER**
**Local**

CyberProof is an extension of customer security team

RESPONSE AUTOMATION

**CYBERPROOF USE CASE MANAGEMENT**
**Detection rules, response actions, and digital playbook creation**

Continuous development of use cases mapped to MITRE ATT&CK

DETECTION CONTENT

**SIEM SECURITY ANALYTICS PLATFORM**
**Sentinel for Cloud Data sources**
**LogRhythm for On-Premise**

Design, configure, monitor, and maintain
Analytics | Correlation | Threat Hunting

LogRhythm · Microsoft Sentinel

ADVANCED DATA ENGINEERING – FILTERING, TAGGING, MASKING, ROUTING TO SECURITY DATA LAKE

**ENDPOINTS & DEVICES**

**SOFTWARE AS A SERVICE (SAAS)**

**HYBRID INFRASTRUCTURE – ON-PREMISES AND CLOUD**

# CyberProof®
A UST Company

## About CyberProof

Fortify your enterprise with cloud security transformation. CyberProof, a UST company, helps enterprises migrate to cloud-native security operations with advanced Managed Detection & Response services that allow you to protect, detect, and respond to new and existing cyber threats faster and more effectively. Our team of nation-state trained experts together with our AI virtual assistant SeeMo challenge the status quo in the cybersecurity industry with a risk-based approach that helps mitigate the potential threat to your business. Our mission is to empower your organization to anticipate, adapt, and swiftly counter cyber threats – with our global security operations centers, in-depth expertise, and a portfolio of services including Tailored Threat Intelligence, Advanced Threat Hunting, Use Case Management, and more. See www.cyberproof.com

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

**cyberproof.com**