

**CASE STUDY:**

# Integrating Azure Sentinel to strengthen detection and exposure management for an industrial supplies organization

**INDUSTRY: INDUSTRIAL SUPPLIES**

## About the client

The client is a major distributor of industrial supplies and is situated in multiple locations across the United States. As a critical supplier to manufacturing, construction, and infrastructure sectors, the organization manages a vast and distributed technology landscape that supports supply chain logistics, e-commerce platforms, and operational systems.

## The client's challenge

The client was interested in scaling security operations across its subsidiaries, and approached CyberProof for support both in developing a next-generation Security Operations Center (SOC) and an enterprise-wide Incident Response (IR) framework designed to shorten time to response and reduce total cost of ownership.

As part of this initiative, the security team sought to improve visibility and consistency across a distributed IT environment while addressing exposure management gaps created by rapid digital transformation. In preparing for the roll-out of the enterprise-wide IR framework, the client's team expressed concern about staffing, running, and tuning an in-house SIEM. They recognized that outsourcing these aspects would help maintain focus on higher-value threat detection and response activities. In addition, the team faced the following challenges:

Establishing an effective onboarding process for security data feeds from the client's operating companies, subsidiaries, and distributed events

Sustaining 24x7 coverage of security operations to ensure continuous threat visibility.

Developing "digital playbooks" and comprehensive SLA, compliance dashboards and reporting to support governance and assurance.

The organization sought a platform that would serve as a single pane of glass for all security technologies, enabling unified threat visibility, faster response, and improved resilience against evolving cyber risks.

## Benefits



**Fewer false positives** with a fully functional SIEM that reduces noise and improves detection fidelity.



**Increased automation of SOC processes**, including prioritization of alerts by severity and SLA level and proactive correlation of threat intelligence sources to accelerate exposure reduction.



**Greater operational efficiency** through the integration of multiple tools to a single pane of glass, enhancing visibility and enabling faster detection and response



**Event data enrichment and insights**, providing context that strengthens triage, identification of attack patterns, and facilitates faster, more effective response.



Ultimately, we selected CyberProof because they showed the greatest desire to partner with us and adapt – as we navigate the unknowns and mature into this space. They aligned with our desire to go after events where they are logged, which will help us onboard sensors quickly and cleanly. We also appreciate CyberProof's advanced automation capabilities and are looking forward to building out the ability to automate more responses over time.

– Client CEO

# The solution

The client made a strategic decision to accelerate its cloud transformation, migrating infrastructure from on-premises environments to Microsoft Azure. As an existing Microsoft Azure customer, the organization viewed Microsoft's cloud ecosystem as the optimal platform for modernizing operations and strengthening security.

To enable a next-generation Security Operations Center (SOC), CyberProof implemented Microsoft Azure Sentinel as the client's cloud-native SIEM, fully integrated with the CyberProof service delivery platform. This integration created a single, scalable environment for threat detection, investigation, and response—reducing exposure across the client's distributed business units and improving overall cyber resilience.

CyberProof designed and deployed the Azure Sentinel environment in alignment with Microsoft's best practices and methodologies, providing expert guidance and operational support to ensure a seamless and secure implementation. Key activities included:

- Enabling and setting up the Azure Sentinel workspace
- Connecting cloud and on-premises data sources for unified visibility

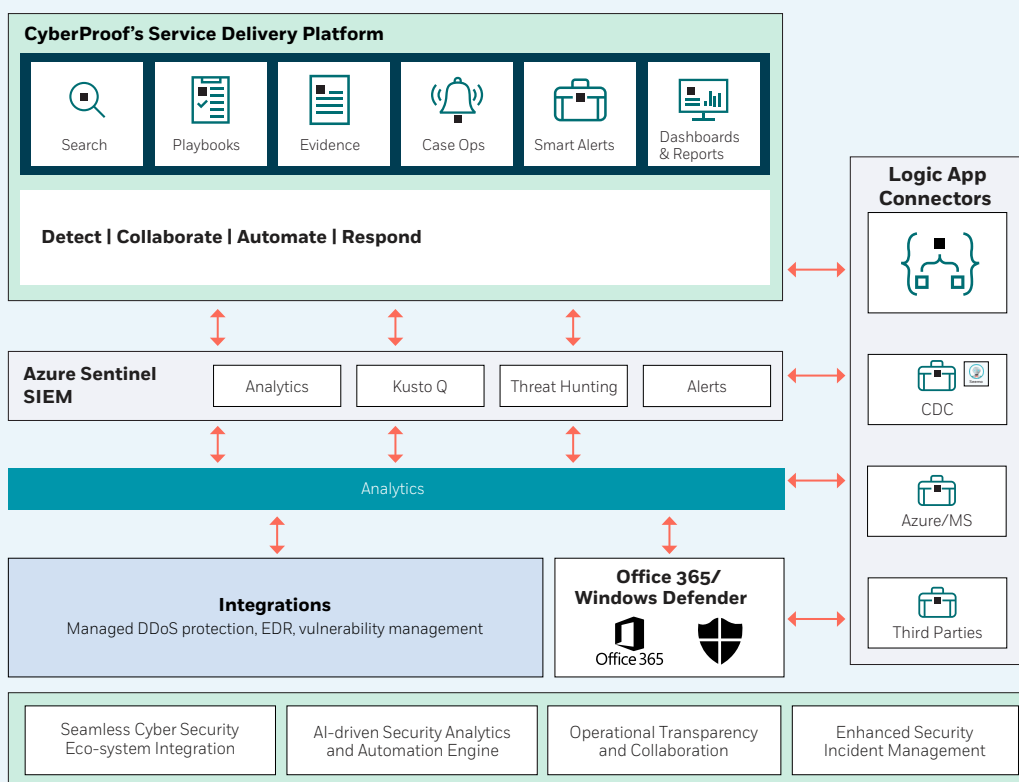
- Configuring use cases and customized playbooks for prioritized threats
- Tailoring dashboards and executive reports for compliance and operational metrics

By integrating Azure Sentinel with the CyberProof service delivery platform, the client gained the benefits of automated detection, incident response, and recovery, as well as enhanced visibility into potential exposure points. The platform's orchestration and automation capabilities enabled continuous threat hunting, streamlined incident triage, and faster remediation cycles.

CyberProof's analysts also leveraged the Microsoft Security Graph toolset, which correlates billions of global security signals in real time, dramatically reducing incident dwell time and improving detection accuracy.

This deployment represented one of the first commercial rollouts of Microsoft Azure Sentinel as a managed service. The new SOC strengthened detection and response capabilities, reduced operational complexity, and improved cost efficiency—empowering the client to respond to security threats faster and more effectively, thereby minimizing the potential business impact of cyber incidents.

## AZURE SENTINEL INTEGRATION WITH THE CYBERPROOF DEFENSE CENTER PLATFORM



## 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