CyberProof®
A UST Company

CASE STUDY:

Security services for a large distributor of industrial supplies

INDUSTRY: RETAIL & MANUFACTURING

cyberproof.com

Client background

The client is a major distributor of industrial supplies and is situated in multiple locations across the United States.

Client challenge

The client was interested in scaling security operations in the company's subsidiaries, and approached CyberProof for help both in developing a next-generation Security Operations Center (SOC) and for assistance with rolling out an enterprise-wide Incident Response (IR) framework designed to shorten time to response and reduce total cost of ownership. In preparing for the roll-out of the enterprise-wide IR framework, the customer's team expressed concern about staffing, running, and tuning an in-house SIEM. They felt that outsourcing these aspects of the implementation process would alleviate pressure on the security team. In addition, the team faced the following challenges:

- Establishing an effective onboarding process for security data feeds from the customer's operating companies, subsidiaries, and distributed events
- Sustaining 24x7 coverage of security operations
- Developing "digital playbooks" and comprehensive SLA, compliance dashboards and reporting

The team sought a platform that would function as a "single pane of glass" for all the various technologies they use.

Benefits

Fewer false positives with a fully functional SIEM that reduces noise

Automating alert prioritization and proactively querying external sources

Greater operational efficiency with a single pane of glass and meeting IEC/ISO and NIST compliance requirements

Event data enrichment and insights with SeeMo, our virtual analyst

> 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**

Our solution

The client decided to aggressively move its infrastructure from on-premises to the cloud, and as an existing Microsoft Azure client, viewed Microsoft Azure as the provider of choice for IaaS and PaaS services. For these reasons, it was important to provide a solution for the customer's new, next-gen SOC that would be fully integrated with Microsoft's native cloud SIEM solution, Azure Sentinel.

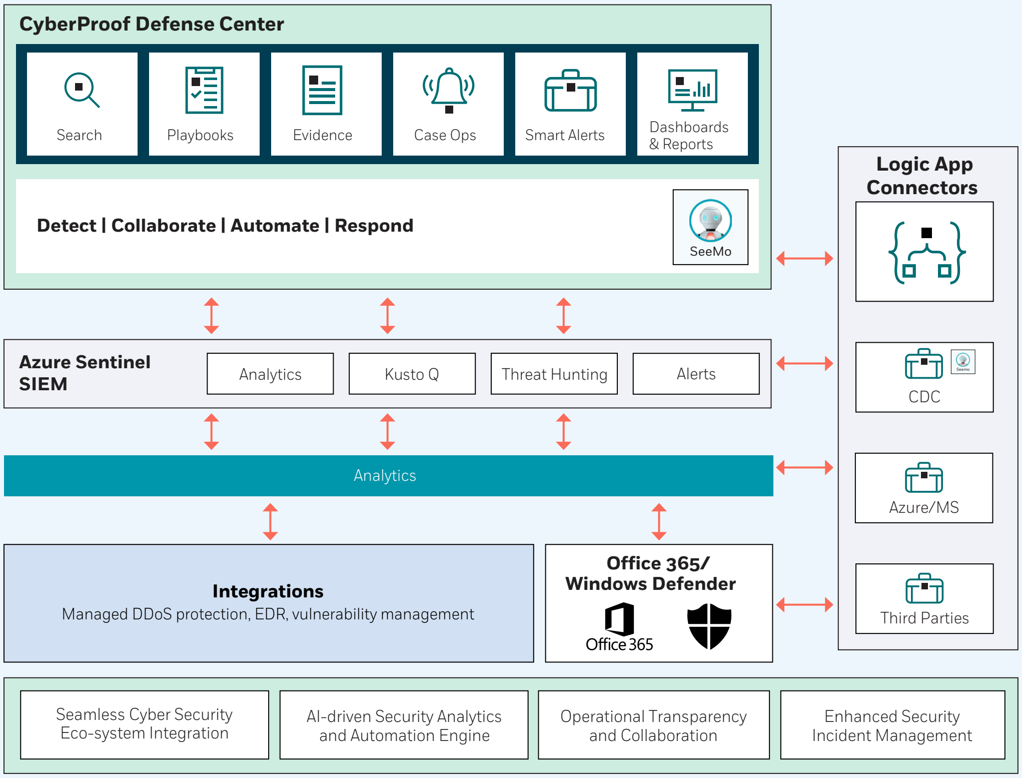
Azure Sentinel is pre-integrated with the CyberProof Defense Center (CDC), so customers can use the cloud-scalable orchestration security operations platform for intruder hunting including automated detection, incident response, and recovery – improving cyber resilience while lowering costs. CyberProof set up the Azure Sentinel environment aligned to Microsoft's best practices and methodologies – providing expert advice and support in setting up a robust security monitoring solution, including:

- Enabling and setting up the Azure Sentinel workspace
- Connecting cloud and on-premises data sources
- Configuring use cases and customized playbooks
- Tailoring dashboards and personalized reports

Furthermore, CyberProof's security team is able to take advantage of the Microsoft Intelligence Security Graph, which helps to dramatically reduce incident dwell time.

CyberProof's deployment for this client is one of the first commercial deployments of the Microsoft Azure Sentinel SIEM to be sold as part of a managed service. CyberProof's deployment of a new, next-generation SOC facilitates effective detection and response, drives operational efficiency, and dramatically reduces the cost and time required to respond to security threats – thereby minimizing the potential business impact of a cyber attack.

AZURE SENTINEL INTEGRATION WITH THE CYBERPROOF DEFENSE CENTER PLATFORM


CyberProof Defense Center
Search
Playbooks
Evidence
Case Ops
Smart Alerts
Dashboards & Reports
Detect | Collaborate | Automate | Respond
SeeMo
Azure Sentinel SIEM
Analytics
Kusto Q
Threat Hunting
Alerts
Analytics
Integrations
Managed DDoS protection, EDR, vulnerability management
Office 365/ Windows Defender
Office 365
Logic App Connectors
CDC
Azure/MS
Third Parties
Seamless Cyber Security Eco-system Integration
AI-driven Security Analytics and Automation Engine
Operational Transparency and Collaboration
Enhanced Security Incident Management

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations. For more information, visit www.cyberproof.com.

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

cyberproof.com