



CASE STUDY:

Threat-led SIEM
transformation delivers
85% cost savings for
international retailer

INDUSTRY: RETAIL

Client Background

Our customer is a leading retailer with more than 1,000 stores across the United States and Canada, serving both consumers and businesses. With extensive digital operations — from e-commerce platforms to point-of-sale systems and complex supply chain networks — the organization manages vast amounts of sensitive customer and transaction data. Retailers remain a prime target for adversaries seeking to monetize stolen data or disrupt operations through ransomware and supply chain attacks.

To strengthen resilience while streamlining operations, the company decided to consolidate its security environment under a single trusted cloud vendor. As an existing Microsoft 365 user, the retailer embraced Microsoft's comprehensive security suite to align its defenses with best-in-class cloud-native solutions.

The challenge

The client faced significant challenges in reducing operational costs while improving the effectiveness of its security operations. Despite having invested in five different SIEM platforms over the past decade, the company continued to struggle with visibility gaps and inefficient data management. These fragmented environments created blind spots, delayed detection, and drove up costs.

The legacy Splunk SIEM was particularly difficult to sustain. Broad data ingestion and retention practices inflated infrastructure and licensing costs while introducing unnecessary noise, making it harder to prioritize genuine threats. This lack of optimization increased exposure to risks such as data theft, ransomware, and insider threats — while also complicating compliance reporting under PCI DSS and SOX requirements.

To address these challenges, the client needed a reliable strategy to migrate to a cloud-native SIEM. Their key objectives for the transformation were:

Cost savings:

Reduce infrastructure, ingestion, retention, and operational overheads without sacrificing visibility into high-priority risks

Optimized design:

Build an intelligent SIEM architecture that ingests only relevant data, improves detection accuracy, and closes existing blind spots

Self-sufficiency:

Gain the expertise and training to empower internal teams to sustain and evolve the platform, ensuring long-term resilience without over-reliance on external providers.

Benefits



85% cost reduction with exposure-led design: A cloud-native, optimized SIEM architecture reduced ingestion, retention, and licensing costs, while ensuring visibility into the threats that matter most.



Autonomy with resilience: Expert training empowered internal teams to maintain and optimize the SIEM, reducing reliance on external vendors while sustaining control over exposure management.



Streamlined risk signal management: An intelligent layer leveraging Cribl and Sentinel prioritized high-value security data for the SIEM, while archiving non-critical data to meet compliance needs.



Stronger visibility and control: The business now has a consolidated, future-ready security stack providing full transparency across business units and reducing blind spots.

Why CyberProof?

Following an in-depth evaluation of three vendors, CyberProof's strong partnership with Microsoft and extensive experience with similar large-scale transformations made it the clear choice for the business.

"We completed a series of technical meetings, and the client immediately recognized our deep understanding of the Microsoft Security Suite," said Jim Nyhan, Director US Enterprise Sales, CyberProof. "They also valued our flexible engagement model. Other vendors wanted to deliver a finished product with little involvement from the client. But the client knew they needed hands-on experience to manage exposures effectively and optimize the platform long-term. CyberProof was the only vendor offering the co-sourced partnership that gave them both expert guidance and the ability to remain in control of their own resilience."

Our Solution

CyberProof led a consultative program of hands-on workshops and working sessions to migrate from Splunk to Microsoft Sentinel in a way that reduced exposure as well as cost. Activities included source evaluation, licensing review, and query translation, plus threat-led use case development and ruleset design that prioritized high-risk scenarios. CyberProof also implemented a custom forwarding solution and a data optimization layer, and built real-time attack scenario queries mapped to adversary behavior to improve time to detect and contain.

CyberProof mobilized specialists in cost-optimized architecture, detection engineering, and automation, organized across consultancy, coaching and learning, and reusable intellectual property. This capability mix ensured the target operating model was threat-led, that content and automation closed visibility gaps, and that exposure management became a measurable, repeatable practice rather than a one-time migration activity.

As part of coaching and learning, to maintain consistency in data processing, the team started with an in-depth discovery of existing rules and content. "The first thing that was clear to us was that they needed guidance over their content strategy and especially their rules, some of which were built for people who weren't even there anymore," Geordie Marin, Use Case Management Team Lead, CyberProof, said. "We had daily calls to analyze, understand and translate 264 detection rules, and then translate them from Splunk SPL to Sentinel KQL, which can't be completed automatically - it needs to be done manually

and requires deep expertise. For the client, it was like multiple crash courses on how to use KQL effectively, including connecting the dots with logs and log schema across other teams. They started with zero knowledge of KQL, and by the end of the process — they were proficient." CyberProof's knowledge base of 5,000+ rules accelerated coverage against relevant TTPs, improving fidelity and shrinking exposure windows while upskilling the client team.



A core design goal was to reduce cost while improving risk signal quality. CyberProof implemented an intelligent telemetry layer using Cribl to prioritize high-value security data for SIEM ingestion and route lower-value data to a lake for archival and compliance. This improved signal-to-noise, preserved investigative depth, and reduced both ingestion and retention costs without increasing exposure.

This architecture materially lowered the cost of retaining mandatory logs while maintaining threat investigation readiness and auditability.

“By using a data lake solution, we could reduce both the ingestion and the retention costs for the client,” Akos

Danis, Senior Security and Cloud Architect, CyberProof, said. “They were ingesting around 1.5-2TB of data each day, which would have a monthly [cost](#) of \$111,600 per month plus \$41,000 monthly for active retention after three months. A data lake is 85% cheaper for ingesting data, and then as they had a regulatory requirement to keep logs for 12 months, we supported them by intelligently sending the right data to ADX for a lower cost. Overall, the client would be charged \$6,000 per month instead of \$40,000 per month for data storage.”

CyberProof’s consultancy and hands-on support ensured that prior investments in reporting and intellectual property were preserved, while reducing compliance exposure. By helping the client transition regulatory reports from Splunk to Sentinel, the solution



maintained audit readiness and avoided costly rework. “At the end of the day, the business has invested decades of their processes and people into previous tools,” Jason Malacko, Director Architecture Strategic Solutions, CyberProof, said. “They don’t want to just throw that away, they want to be able to take the reports they had for compliance with regulations like PCI-DSS and Sarbanes-Oxley in Splunk, and recreate them in Sentinel. We brought in all the requisite experts to make that happen, from report writers to architects and engineers so that we could preserve those investments.”



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