CyberProof®
A UST Company

CASE STUDY:

A Leading Retail Company Reduces Data Costs by 85% with SIEM Transformation from CyberProof

INDUSTRY: RETAIL

CLIENT BACKGROUND

Our customer operates a network of 1000+ retail stores across the United States and Canada, providing a wide range of products and services to consumers and businesses.

Previously relying on disparate solutions for security and a hybrid architecture, the business had decided to consolidate under a single, experienced cloud vendor. As an existing Microsoft 365 user, and recognizing Microsoft's industry-leading cloud security suite, they chose to embrace the whole security stack, making a commitment to Microsoft products and services.

THE CHALLENGE

As part of their wider shift to adopt the Microsoft suite of products, and to meet aggressive cost-cutting goals, our client needed support in migrating from an on-premises Splunk SIEM to cloud-native Microsoft Sentinel. Over the previous decade, the business had attempted five different SIEM solutions, and was looking for a strategic partner to ensure that this migration was successful.

Goals for the SIEM transformation included:

Cost savings:
As well as the inherent cost savings of becoming cloud-native and consolidating under a single vendor, the business wanted to reduce data costs, and limit the overhead related to operations and infrastructure maintenance.

Intelligent design:
With many moving pieces to consider, the business needed a smart solutions design, specifically around data ingestion and logging. Expertise and a strong track record with SIEM transformation was crucial.

An emphasis on learning:
The business did not want a vendor who would take the migration off their hands and present them with a finished solution. They were looking for a strategic partner that could teach them how to maintain their own infrastructure.

BENEFITS

85% cost reduction by design: A cloud-native, optimized design eliminates many of the ancillary costs including infrastructure and maintenance, on top of reduced data ingestion, retention, and licensing fees.

Autonomy over maintenance and optimization: The business can now take ownership over their SIEM migration, after being empowered by dozens of hours of in-house training from an expert Microsoft partner.

Streamlined data management: An intelligent layer in the solutions design leverages Cribl and Sentinel to channel only relevant security data to the SIEM, archiving the rest for compliance purposes.

Enhanced peace of mind: The business now has complete visibility and control over security operations, and a future-focused security stack consolidated across business units.

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 we could see that the client really appreciated our deep understanding of, and technical proficiency in the Microsoft Security Suite," Jim Nyhan, Director US Enterprise Sales, CyberProof, said. "They also loved our flexible engagement model. Other vendors wanted to do the whole product implementation alone and then hand it back to the client. But the client wanted to do the hands-on work themselves, with consultative support and involvement from an expert co-sourced partner. They knew that they were the ones who would have to optimize it, and to work with it day-in and day-out. If they were just handed a finished product, they wouldn't be able to look after it autonomously. CyberProof was the only vendor offering the partnership they needed."

OUR SOLUTION

Through a consultative relationship, multiple hands-on workshops in-house, and regular team meetings, CyberProof supported the client with their transformation from Splunk to Sentinel. This included everything from evaluating data sources, reviewing licensing, and translating query languages, to developing use cases and planning rulesets, log collections, and alert preferences. In addition, the process included creating a custom forwarding solution and intelligence and data optimization layer, and building out real-time attack scenario queries to mitigate attacks.

To manage the migration, CyberProof was able to offer an array of personnel with specialist expertise, with skills across diverse areas including cost optimizing architecture, detection engineering, automation, and more. As well as technical expertise, the business was provided with services across three main verticals — consultancy, coaching and learning, and intellectual property.

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." As CyberProof has a knowledgebase of more than 5,000 rules documented, this intellectual property also allowed for intelligent and efficient placement of rules where relevant and where they would have an impact.

Crucially, one of the consultancy goals of the transformation was to create a way to reduce data costs and improve data management. Before working with CyberProof, the business was sending all of their data to Splunk, but the cost was prohibitive. Instead, as part of the transformation, CyberProof supported the company in placing an intelligent layer into the solutions design via Cribl, so that the business could handle the data load seamlessly, and also be more judicious — sending only meaningful security data to the SIEM, and sending other data to a data lake for archiving and compliance purposes.

"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."

The expert consultancy and hands-on support also allowed the business to retain their previous investments in reporting and intellectual property. "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 delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security, delivers industry-leading security 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

cyberproof.com