



**CASE STUDY:**

Financial services organization reduces threat exposure and lowers security data costs by millions

**INDUSTRY: BFSI**

## Client background

A large, multinational company approached CyberProof to strengthen its security operations through a more threat-led and exposure-aware approach. The company operates in around 50 countries worldwide, with a complex digital footprint. The client's goal was to ensure business operations remain secure by transforming the firm's current cyber practices to better identify, prioritize, and reduce material threat exposure – and by establishing an innovative, next-generation cyber security SOC operation.

## Client challenge

In its search for a security solution, the client was not looking for a traditional Managed Security Services Provider (MSSP) focused solely on alert handling and tool operation. The firm was seeking a partner willing to work in a hybrid model, where cloud and on-site resources and assets could be jointly assessed, monitored, and prioritized based on threat exposure. In selecting a partner who could meet the firm's security needs, the client defined the following main objectives:

- Adoption of a more holistic, threat led, and risk-based approach to threat detection and response that prioritizes the most critical exposures and attack paths.
- Integration of orchestration and automation platforms that enable faster validation, containment and mitigation of threats to **minimize business impact**.
- Development of streamlined SOC processes and innovative tools that improve analyst efficiency while reducing noise and unmanaged exposure
- Implementation of a cloud-native SIEM platform to cover a hybrid cloud and on-premises architecture enabling scalable visibility across the evolving attack surface.

## Benefits



**Lower security data costs:** Reduced log ingestion and storage costs by aligning data collection to threat relevance.



**Higher signal, less noise:** Fewer false positives through improved correlation and contextualization across sources.



**Greater operational efficiency:** Cloud-native and hybrid deployment accelerates detection and response through automation.



**Faster exposure reduction:** Orchestration and automation shorten time to response and reduce material risk.



This is probably the biggest Sentinel deployment in the world right now. CyberProof's scalable, cloud-native services delivered through their CDC platform provide us with a transparent and collaborative hybrid SOC environment.

- Head of Cyber Defense

# The solution

CyberProof’s deployment for this client includes one of the first commercial deployments of the [Microsoft Sentinel cloud SIEM solution](#). Sentinel supports data collection for on-premises, hybrid, and multi-cloud ecosystems, with intuitive dashboards and reporting that provide continuous security and intelligence insights.

CyberProof’s team in Paris, Tel Aviv, and Trivandrum (India) works as an extension of the client’s security team and functions as an integral part of their threat reduction objectives.

CyberProof helped dramatically reduce the cost of log ingestion and storage as the client migrated to [cloud-native security operations](#), leveraging Azure Data Explorer (ADX) together with the CyberProof Log Collection (CLC) tool. By moving the long-term retention of the logs, and the processing of custom collected logs – the “heavy lifting” – over to ADX, CyberProof was able to manage massive quantities of data for the client, at a radically lower cost.

CyberProof also deploys a full range of co-managed cybersecurity services for the client, including:

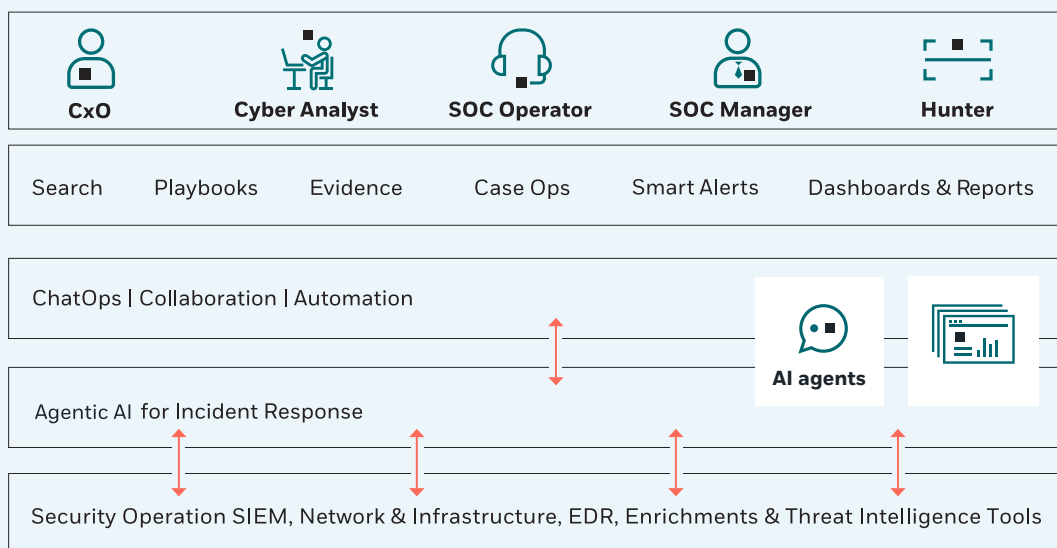
- 24/7 event monitoring, event enrichment, and triage
- Incident response with customized threat detection rules, use cases, and digital playbooks
- Detection engineering

CyberProof provides other advanced SOC services, such as [targeted threat intelligence](#), managed Endpoint Detection and Response (EDR), and [vulnerability management](#).

CyberProof helps automate cyber operations within the service delivery platform – enriching event data, proactively querying external sources, responding to analysts’ requests by providing contextualized and actionable information, automatically creating incidents without human intervention (based on collation and context), and automatically executing non-intrusive steps in digitized playbooks. By automating tier 1 and 2 activities, CyberProof’s SOC helps reduce false positives and shrink dwell time.

Analytics and deep learning techniques enable the handling of high data volumes and the detection of both known and emerging threats, allowing the SOC to focus on the exposures that matter most.

As a result of the cloud migration and the adoption of threat-led, automated security operations, the client significantly reduced security data ingestion and storage costs while improving detection quality and response speed. Automation and analytics reduced false positives, shortened dwell time, and improved visibility across the threat landscape, enabling faster exposure reduction and more resilient security operations.



**SERVICES ARCHITECTURE**

## 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