CyberProof®
A UST Company

CASE STUDY:

Advanced MDR services for a multinational financial services company

INDUSTRY: BFSI

Client background

A large, multinational company approached CyberProof for assistance with their security operations. The company operates in multiple countries worldwide.

Client challenge

The client's goal is to ensure business operations remain secure by transforming the firm's current cyber practices – and establishing an innovative, next-generation cyber security SOC operation.

In its search for a security solution, the client was not looking for a traditional Managed Security Services Provider (MSSP). The firm was seeking a partner willing to work in a hybrid model, where cloud and on-site resources and assets would complement each other. In selecting a partner who could meet the firm's security needs, their main objectives included:

- Adoption of a more holistic and risk-based approach to threat detection and response to increase security resilience
- Integration of orchestration & automation platforms that allow threats to be detected and mitigated to minimize business impact
- Development of streamlined SOC processes and innovative tools that drive operational efficiencies and reduce costs
- Implementation of a cloud-native SIEM platform to enable a hybrid cloud and on-premises architecture

Benefits

Fewer false positives as data and logs are collected from multiple sources, reducing errors and time to detect

Cloud-native and hybrid deployment providing greater operational efficiency, by leveraging cloud-native tools and automations

Reduced risk with orchestration & automation capabilities that provide faster time to response and increased visibility

Single view supporting multi-team SecOps collaboration, with real time alerts and recommendations

Extended security monitoring for Office 365 and other web applications

> 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**

Our solution

CyberProof's deployment for this client includes one of the first commercial deployments of the Microsoft Azure Sentinel Security Information and Event Management (SIEM) solution. Azure Sentinel supports datacollection for on-premises, hybrid, and multi-cloud ecosystems, with intuitive dashboards and reporting that provide continuous security and intelligence insights.

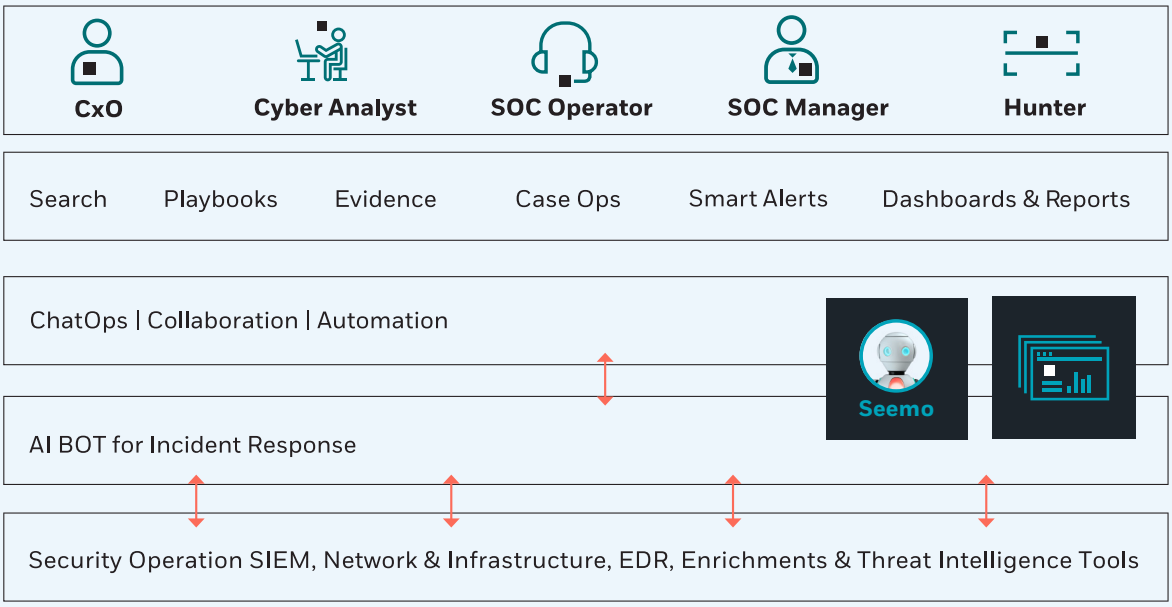
CyberProof's team in Paris, Tel Aviv, and Trivandrum (India) works as an extension of the customer's security team and functions as an integral part of their threat reduction objectives. CyberProof deploys the full range of managed cybersecurity services, including:

- 24/7 event monitoring, event enrichment, and triage
- Incident response with customized threat detection rules, use cases, and digital playbooks
- Use Case Factory that is fully integrated with the CyberProof Defense Center (CDC) platform

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 CDC – 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 some of the SOC's tier 1 & 2 activities, the CDC helps reduce false positives and shrink dwell time, i.e., the period beginning when a threat actor has undetected access to a network and ending when a threat is completely removed.

The CDC leverages analytics and deep learning algorithms, which are key in handling huge volumes of data in order to detect and elevate indications of threats (both known and unknown). These capabilities allow the client to accelerate its response and handle emerging threats fast enough to assure the resilience of its systems.



SERVICES ARCHITECTURE

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 | Paris | Singapore | Tel Aviv | Trivandrum

cyberproof.com