CyberProof®
A UST Company

CASE STUDY:

# Security services for a large, financial services company

INDUSTRY: BFSI

cyberproof.com

# Client Background

The client is a financial asset management company with a large IT presence and a broad, international customer base. The client turned to CyberProof to define a defense strategy and fully build out custom cyber defense operations.

# Client Challenge

The client underwent a demerger process from a large, international banking group. Prior to the demerger, the client's entire IT and cyber services were being managed by the holding company.

After the demerger, these services became the cclient's responsibility. The client sought a trusted vendor who could quickly transition their security monitoring service without any disruption to business operations. The client also wanted our help in defining a cyber defense strategy and building fully customized cyber defense operations.

CyberProof was selected as the preferred provider to build and operate the following capabilities and services:

- Security Event Monitoring and Response
- SIEM Platform and Content Management
- Tailored Threat Intelligence
- Incident Response Retainer
- Endpoint Detection and Response
- Vulnerability Assessment and Penetration Testing
- Security Specialists and SMEs as Staff Augmentation

In searching for a partner that could provide end-to-end support, the customer felt that CyberProof was the right fit to meet their existing and future needs, with the ability to leverage the scale and capabilities of its parent organization, UST.

# Benefits

**Single pane of glass view** for analysts providing real-time alerts and recommendations for IT and security incidents

**Quicker response** as the SeeMo virtual analyst combined with our human cyber analysts cut the client's time to respond by leveraging orchestration & automation and providing patch management assistance

**Greater operational efficiency** through the effective integration and orchestration of multiple tools

**Improved visibility into operational activities** by leveraging the platform's collaboration and automation abilities to dramatically reduce response time

# Our Solution

CyberProof set up a new security event monitoring infrastructure and seamlessly transitioned existing configurations, policies, and data – ensuring service continuity. A number of existing security tools were transitioned, ensuring that the client's existing investments were maintained while optimizing and enhancing their capabilities.

CyberProof built additional capabilities leveraging specialist tools, technologies, and processes supported by expert resources to further enhance the client's cyber detection and response abilities.

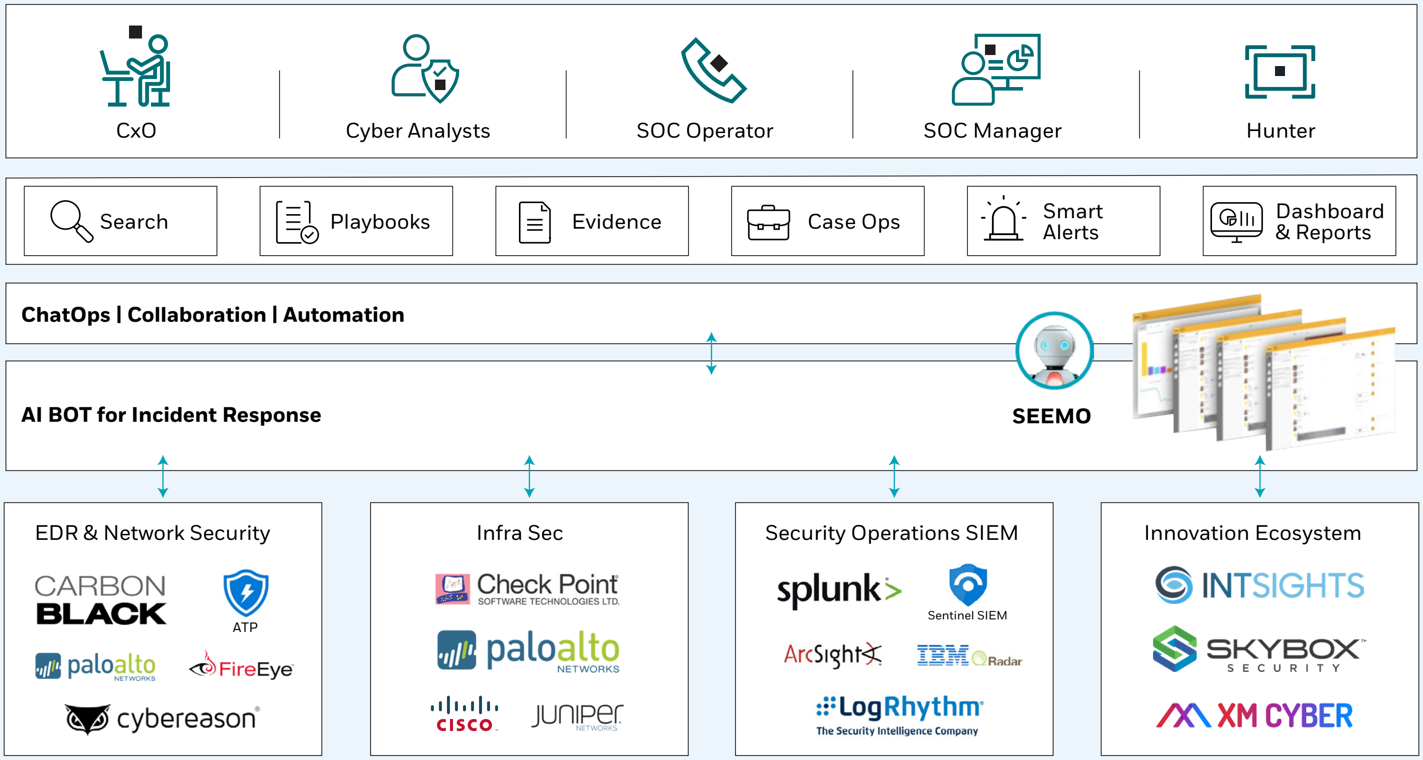
The CyberProof Defense Center (CDC) platform was used to ensure the orchestration of tools including Security Information and Event Management (SIEM), Endpoint Detection & Response (EDR), and Cyber Threat Intelligence (CTI) solutions. This provided the client with a consolidated and prioritized view of enriched alerts and validated incidents – enabling the operations team to act on real issues faster and make data-driven decisions. The CDC platform's ChatOps and automation features provided the client's security staff with a collaborative environment to communicate seamlessly with internal teams and our analysts in real-time when needing to solve complex issues.

The team deployed a range of managed security services to enhance the client's cyber defense capabilities – covering security event monitoring and response, advanced threat intelligence, incident response, and penetration testing.

CyberProof's deployment for this client also included implementing and managing log analytics software to search, analyze and visualize machine-generated Big Data for endpoint protection, detection, and response and external security threat intelligence.

CyberProof provided the client with a single pane of glass with real-time alerts, validated incidents and response recommendations – providing consistency across many different applications. The solution improved the client's operational efficiency and reduced Mean Time to Detect and Mean Time to Respond, improving their cyber security readiness.

## CDC PLATFORM ARCHITECTURE



CxO | Cyber Analysts | SOC Operator | SOC Manager | Hunter

Search | Playbooks | Evidence | Case Ops | Smart Alerts | Dashboard & Reports

**ChatOps | Collaboration | Automation**

**AI BOT for Incident Response**

**SEEMO**

EDR & Network Security

Infra Sec

Security Operations SIEM

Innovation Ecosystem

* The technology stack is illustrative only.

The client had experienced challenges in hiring and retaining skilled staff. CyberProof built a staff augmentation model to provide continuous access to security specialist resources, and functioned as a full partner in helping provide complete end-to-end cyber support and assisting with cloud and digital transformation.

## 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**

© 2023 CyberProof Inc. All Rights Reserved.