CyberProof®
A UST Company

CASE STUDY:

Integrated NOC/SOC services for a large insurance company

INDUSTRY: BFSI

Client background

The client is a large insurance carrier with offices in multiple locations.

Client challenge

The client initially turned to CyberProof after having issues with their previous service vendor, who was providing security alerts but conducting no real triage.

The client's team didn't feel the vendor understood the environment; and the customer's team had to teach the vendor how to use their SIEM solution. This meant that security operations were never fully optimized to their environment and system patching was consistently behind schedule.

Furthermore, the client wanted to be proactive, and wanted the ability to recognize, respond, and recover from attacks more quickly. They felt they needed a platform that introduced automation into security operations.

Benefits

Reduced costs - A lower head count with the new, integrated operations center.

Fewer false positives - Splunk is a fully functional SIEM system, reducing noise and false positives.

Single view for analysts - Provides alerts & recommendations for IT and security incidents.

Quicker response - Our virtual analyst SeeMo and human analysts leverage automation & orchestration and provide patch management assistance.

> We were impressed with the cyber assessment results, which were completed in just three weeks. The talent CyberProof has is real – and that was very clear from our first interaction. After just four weeks of CyberProof working on site, we learned more than we had learned with our previous service vendor after years of working together.
>
> **– Client CEO**

Our solution

CyberProof fused the client's SOC and NOC into a fully-integrated Operations Center, in which tier 1 and tier 2 analysts cover both security and IT tasks.

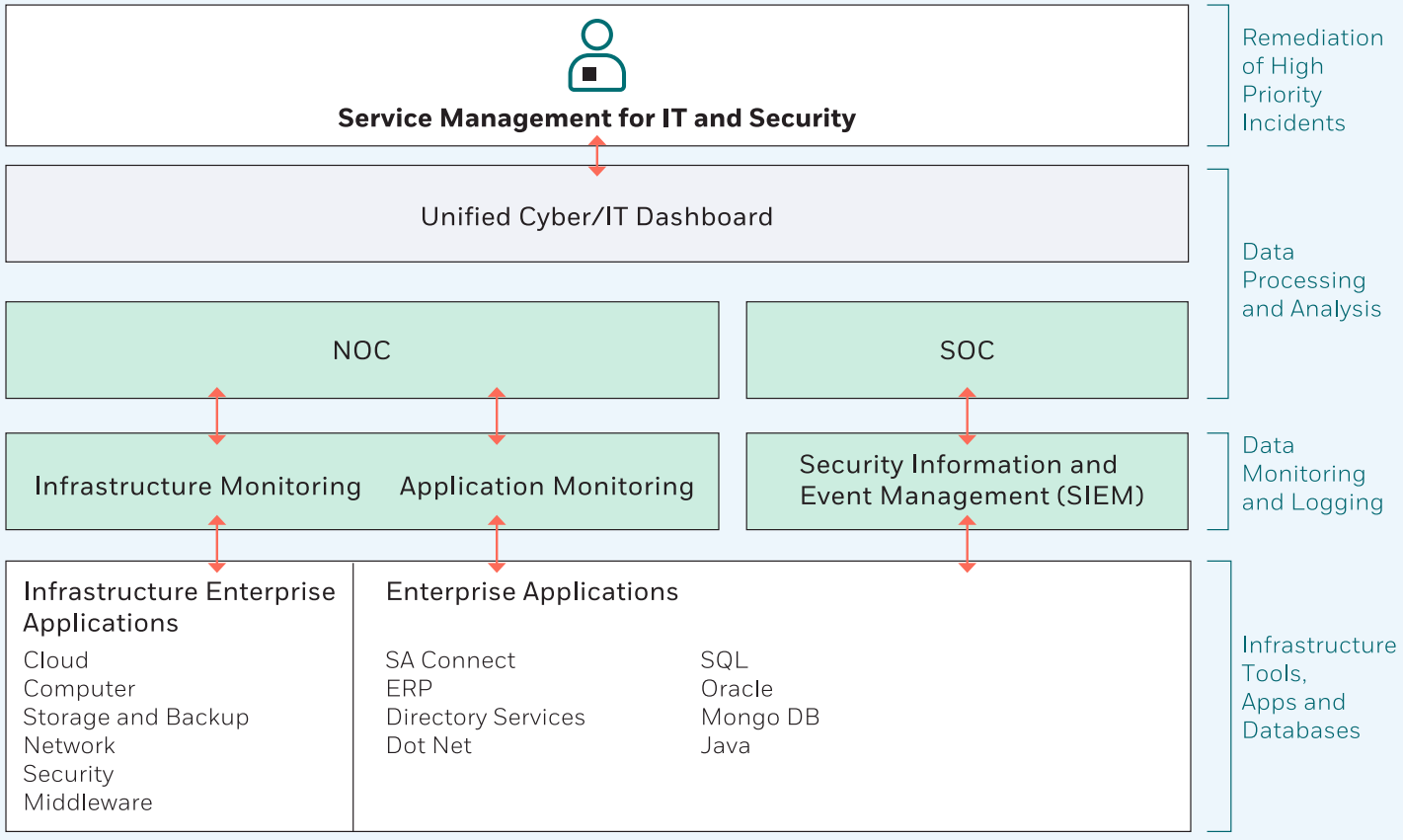
CyberProof also provided the client with a single pane of glass that provides a holistic picture of the customer's security and network environments.

With the implementation of the new platform, the client was able to streamline their staffing from having two separate teams to having a single team for both security and network monitoring. The CyberProof operations team includes an on-site team working Monday through Friday; ten people in India supporting the client 24/7; and tier 3 and 4 support provided by the team in Israel.

In the initial stages of engagement, CyberProof provided an in-depth Cyber Assessment. CyberProof evaluated how the Splunk SIEM solution was being used, provided recommendations, and helped the client optimize the system. We set up new rules and made sure all systems were feeding logs to Splunk.

Today, the CyberProof Defense Center is fully integrated with the system, SeeMo (our virtual analyst) is providing live insights, and we continue to provide the client with threat intelligence on an ongoing basis. CyberProof was able to assist the client in meeting their goals of cutting their head count, reducing costs, and obtaining a single pane of glass for both IT network and cyber security – thereby optimizing their security readiness.

NOC/SOC INTEGRATED 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