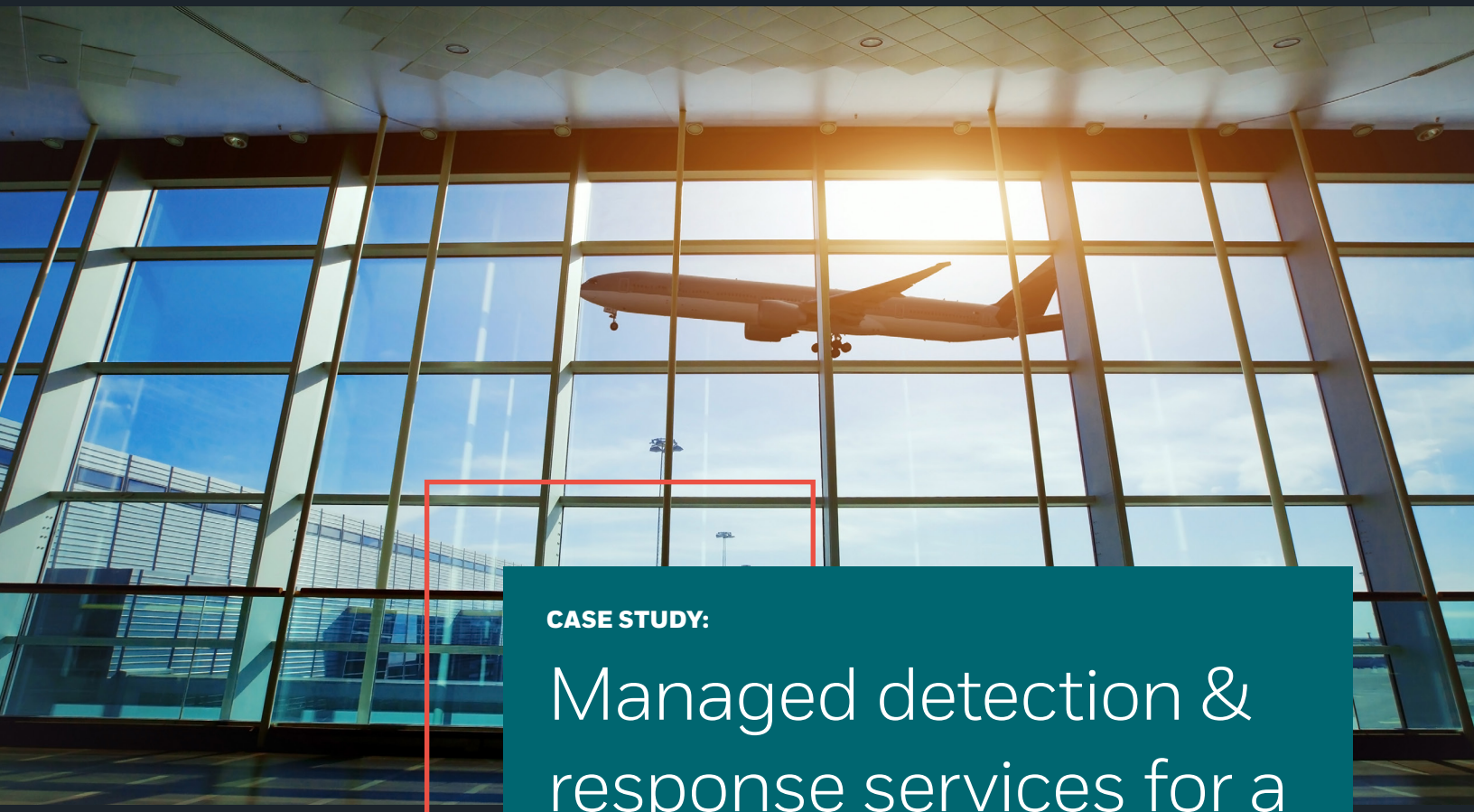
CyberProof®
A UST Company



CASE STUDY:

Managed detection & response services for a world-class airline

INDUSTRY: AVIATION

Client background

The client is one of the world's top airlines. It operates flights serving over eighty international destinations in more than thirty countries.

Client challenge

The airline must ensure round-the-clock safety and security for all its operations. The client's IT ecosystem includes a combination of on-premises and cloud architecture, e-commerce, third-party hosting, application access and management, endpoints, and more.

The client planned to migrate some services and applications to the cloud, potentially exposing systems to new threats – and creating risks and vulnerabilities that they would need to respond to.

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

- Migrating security services from the incumbent service provider
- 24x7 monitoring and response of security events
- Content re-build and ongoing management of the SIEM platform
- Regular threat intelligence updates
- On-site security specialists who provide real-time support

Benefits

Single pane of glass view
Providing real-time alerts and recommendations for IT and security incidents

Quicker response
Using SeeMo, our virtual analyst, combined with our human cyber analysts

Greater efficiency
By optimizing how multiple tools are integrated and orchestrated

Improved visibility
By leveraging the platform's automation and collaboration capabilities to reduce the client's Time to Respond

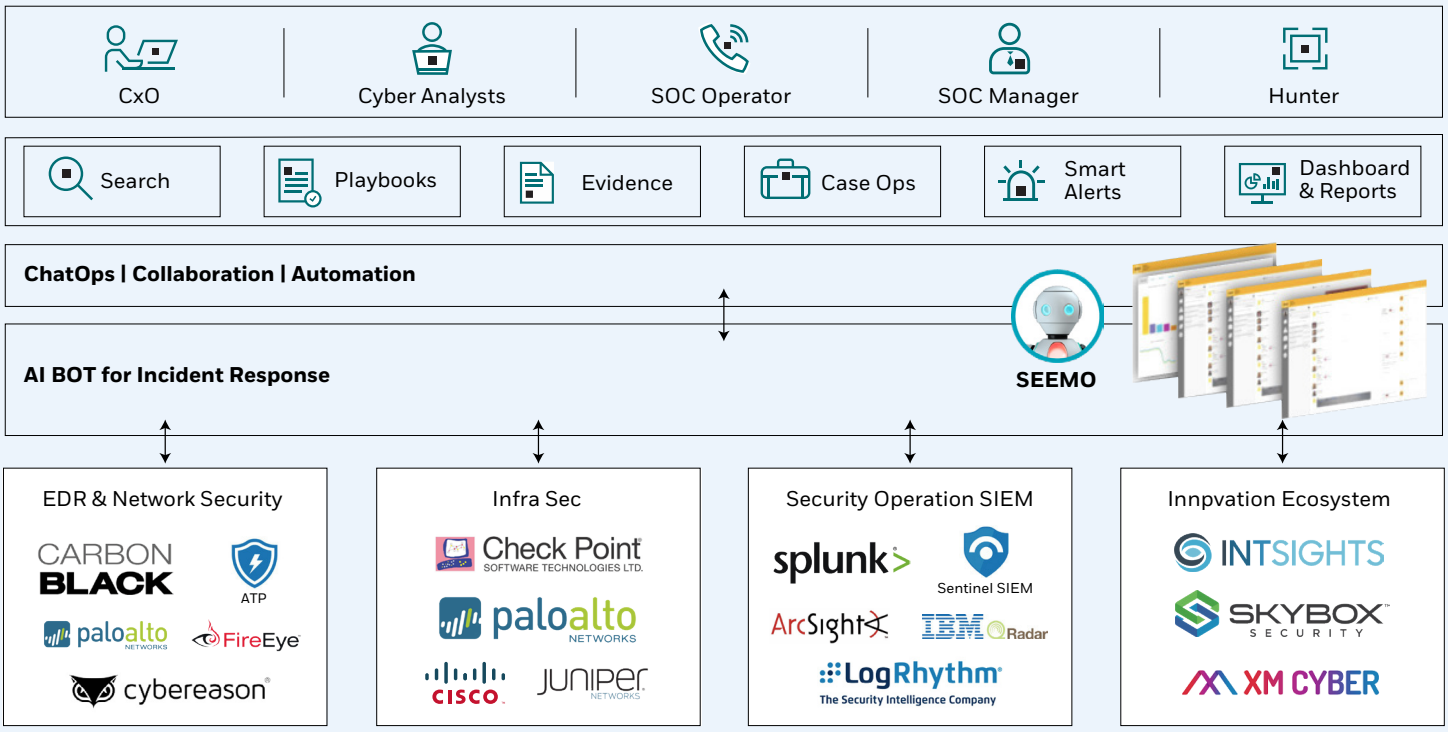
Our solution

CyberProof enhanced the client's Security Information and Event Management (SIEM) infrastructure and seamlessly transitioned existing configurations, policies, and data, ensuring the client's service continuity. New security tools and corresponding log sources were added so that the client's environment was further protected, while CyberProof continued to optimize and enhance their capabilities.

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

Our team onboarded new security devices and set up new detection rules.

CDC PLATFORM ARCHITECTURE



The CyberProof Defense Center (CDC) platform is a single pane of glass that was used to ensure the orchestration of the client's tools, including: Security Information and Event Management (SIEM), Endpoint, and Cyber Threat Intelligence (CTI). This provided the client with a consolidated and prioritized view of enriched alerts and validated incidents, and enabled the operations team to respond to real issues faster and make data-driven decisions. The CDC platform's ChatOps and automation creates a collaborative environment in which internal teams communicate seamlessly with our analysts in real-time, when solving 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, and incident response, where required. Our solution improved the client's operational efficiency and reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), improving cyber security readiness.

The client had previously experienced challenges in hiring and retaining skilled staff. For this reason, CyberProof built a staff augmentation model which provides continuous access to security specialist resources. Our model allows us to function as a full partner in helping provide complete end-to-end cyber support and assisting with cloud and digital transformation.

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 | Singapore | Tel Aviv | Trivandrum

cyberproof.com