

CASE STUDY:

Building a proactive
detection and exposure
management model
for a leading global
airline

INDUSTRY: AVIATION

Client background

The client is one of the world's leading airlines. It operates more than 20,000 flights each month, serving over eighty international destinations in more than thirty countries.

With a highly connected digital ecosystem, 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. Maintaining visibility and managing exposure across a hybrid IT environment is critical. Ensuring continuous protection of mission-critical systems and sustaining cyber resilience remain top priorities for the airline's security leadership.

Client's challenge

The airline planned to migrate key services and applications to the cloud, introducing potential exposure to new threats and increasing the complexity of its security landscape. Maintaining continuous protection across on-premises and cloud environments, while managing multiple third-party integrations, required a more proactive and unified detection and response approach.

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

- Migrating security services from the incumbent service provider
- 24x7 monitoring and response for security events
- Content rebuild and ongoing management of the SIEM platform
- Regular threat intelligence updates aligned to relevant attacker activity
- On-site security specialists providing real-time support and operational continuity

The client's goal was to modernize its security operations with a threat-led, managed detection and response model, improving visibility, accelerating incident response, and reducing overall exposure to emerging risks.

Benefits



Single pane of glass view:

Providing real-time alerts and prioritized recommendations for IT and security incidents, improving visibility into potential exposure points



Quicker response:

Using advanced automation within the CyberProof service delivery platform reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).



Greater efficiency:

By optimizing how multiple tools are integrated and orchestrated, repetitive tasks were automated and resources could be focused on genuine threats.



Improved visibility:

Leveraging the platform's automation and collaboration capabilities, the client enhanced situational awareness and reduced Mean Time to Respond (MTTR).

Our solution

CyberProof enhanced the client’s Security Information and Event Management (SIEM) infrastructure and executed a seamless transition from the incumbent service provider. The migration ensured full continuity of service while improving visibility across on-premises and cloud environments. New log sources and security tools were onboarded, and configurations, policies, and detections were optimized to strengthen coverage and reduce potential exposure.

CyberProof implemented a threat-led approach, aligning detection content and playbooks to the airline’s most relevant adversaries and attack techniques. Regular threat intelligence updates were integrated into daily operations, providing proactive visibility into emerging risks targeting the aviation sector.

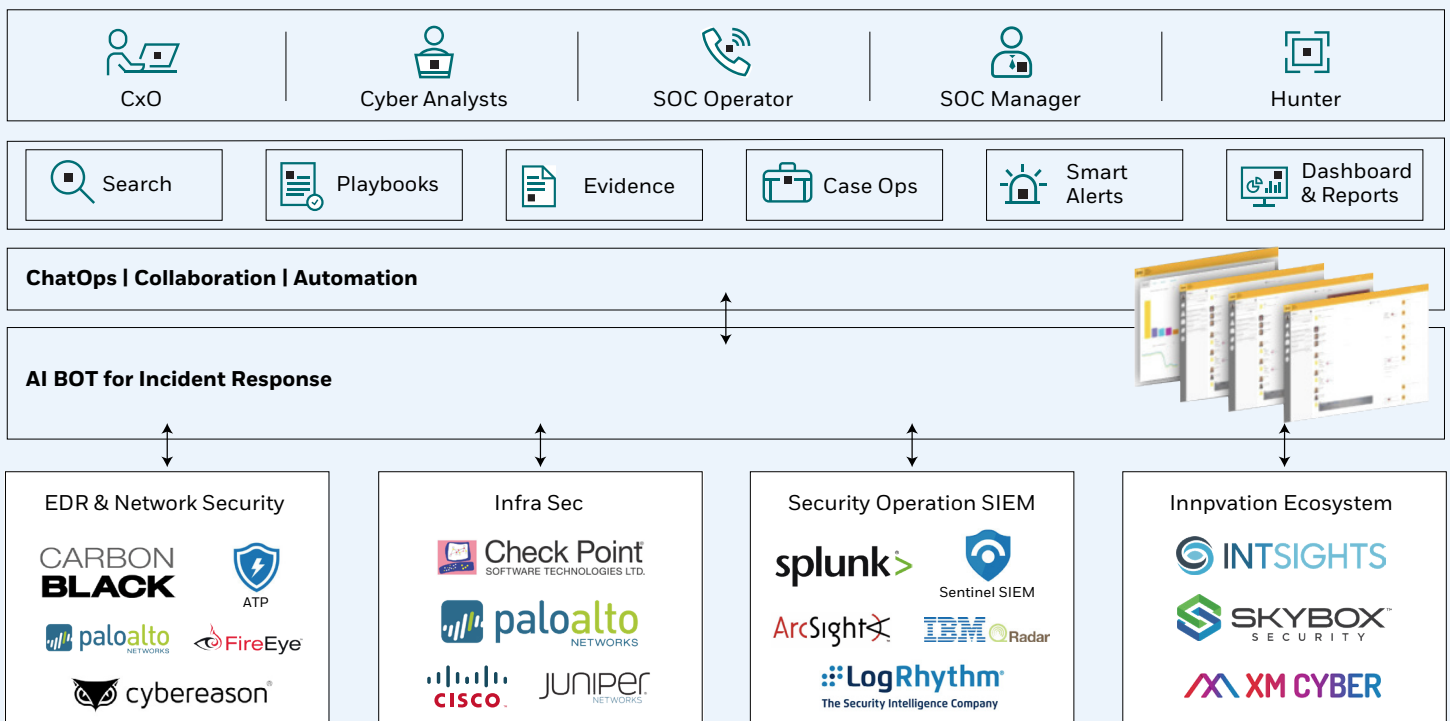
The solution was delivered through CyberProof’s service delivery platform, a unified “single pane of glass” that orchestrates all key security tools, including SIEM, endpoint detection, and threat intelligence systems. This centralized view enables analysts to focus on validated

threats, prioritize alerts based on business risk, and respond faster to incidents. The CDC platform’s ChatOps and automation capabilities also fostered real-time collaboration between CyberProof analysts and the client’s internal security team, accelerating investigation and resolution.

To further strengthen operational resilience, CyberProof deployed managed detection and response services covering 24x7 monitoring, threat intelligence, and incident response. These capabilities significantly improved Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), helping the client maintain continuous situational awareness and a proactive exposure management posture.

Finally, recognizing the challenges of hiring and retaining skilled staff, CyberProof implemented a staff augmentation model that provides continuous access to expert security resources. This partnership approach ensures the airline maintains advanced detection and response capabilities while supporting its broader cloud and digital transformation initiatives.

CYBERPROOF’S SERVICE DELIVERY PLATFORM



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.

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum