



CASE STUDY:

Integrated NOC/SOC delivers threat-informed visibility for insurance sector

INDUSTRY: BFSI

Client background

The client is a leading U.S.-based insurance provider with offices across multiple states. The organization serves both individuals and businesses, offering a wide range of property, casualty, and specialty insurance products. As a major player in the financial services sector, the client operates in a highly regulated environment, where data security, system resilience, and customer trust are paramount.

Client challenge

The client's prior vendor provided a high volume of alerts with little triage or contextualization, leaving the internal security team to separate real threats from noise. This lack of prioritization meant exposures went unresolved, system patching lagged behind, and critical risks persisted.

In addition, the vendor lacked a deep understanding of the client's environment, forcing the client's team to guide them on how to use their own SIEM platform. As a result, threat detection and response remained reactive and inefficient.

The client wanted to move beyond reactive alerting to a threat-led operating model — one that would reduce noise, identify exposures in both IT and network environments, and accelerate the ability to recognize, respond to, and recover from cyberattacks. Their goal was to integrate automation and contextual intelligence into operations, improving resilience against adversaries targeting the insurance sector, including ransomware operators and fraud-focused cybercriminals.

Benefits



Holistic visibility: Single pane of glass across IT and network environments



Reduced exposure: Optimized SIEM rules to prioritize relevant threats and reduce false positives



Faster response: Automation and global 24/7 coverage accelerate containment



Stronger resilience: Defenses aligned to ransomware and fraud adversary tactics



We were impressed with the cyber assessment results, which quickly highlighted critical exposures we hadn't seen before. CyberProof's team brought real expertise from day one, and within weeks we had clearer visibility of our risks and stronger defenses than we'd achieved with our previous vendor in years."

— Client CEO

The solution

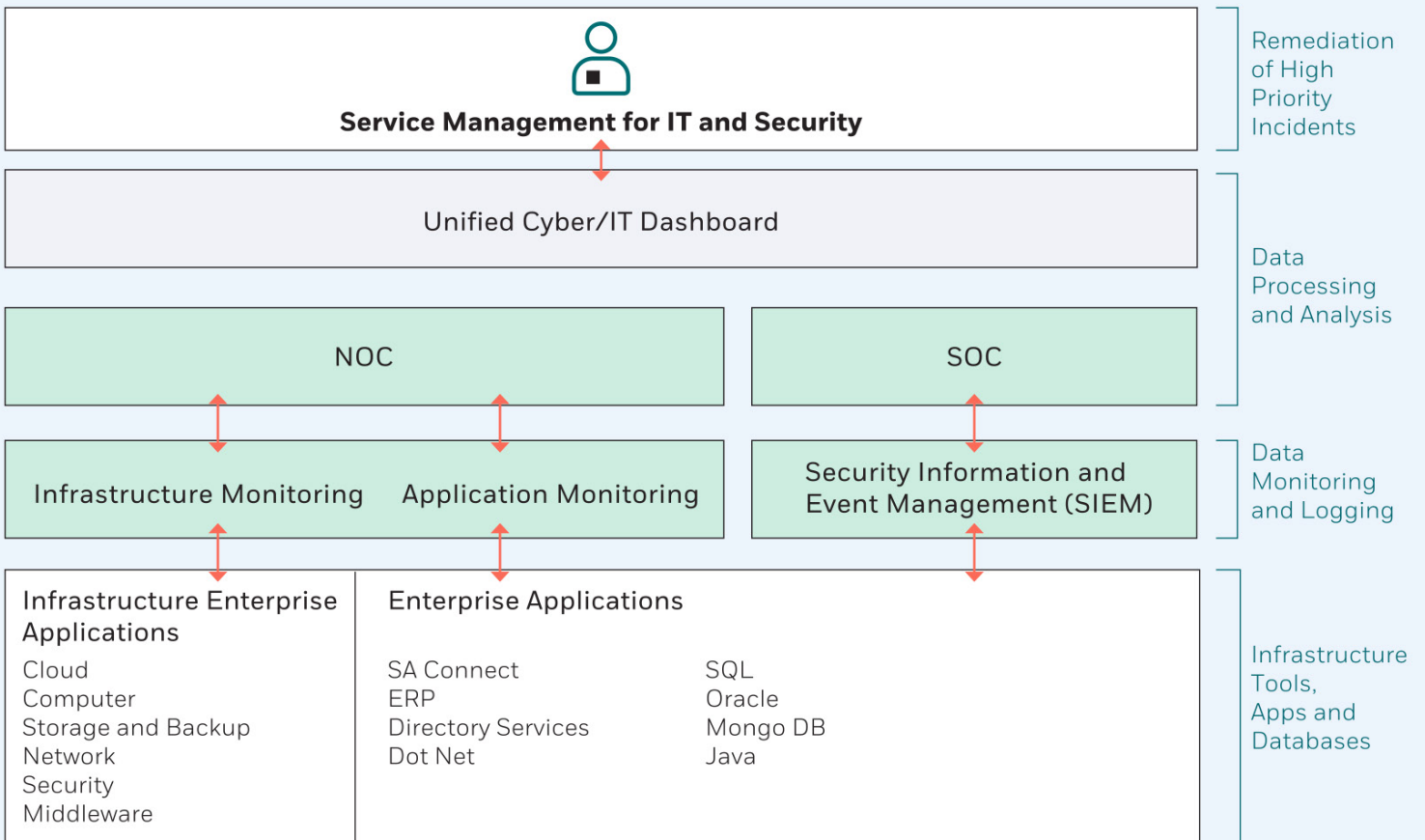
CyberProof unified the client’s SOC and NOC into a fully integrated Operations Center, giving analysts a single pane of glass that delivered a holistic, threat-informed view of both security and network environments. This integration reduced silos, eliminated duplication of effort, and ensured exposures could be identified and remediated across IT and network assets.

As part of the transformation, CyberProof conducted a Cyber Assessment to optimize the client’s Splunk SIEM. New rules and log integrations ensured that monitoring focused on the most relevant threats, reducing false positives and strengthening resilience against ransomware and fraud campaigns targeting the insurance sector.

Staffing was streamlined by consolidating two separate teams into one integrated function for both security and network monitoring. CyberProof provided a global delivery model: an on-site team working Monday through Friday, a 24/7 operations team in India, and advanced tier 3 and 4 support from Israel. This ensured continuous monitoring, rapid response, and proactive exposure management.

Automation played a central role. CyberProof’s service delivery platform, combined with expert human analysts, enriched alerts with contextual threat intelligence, accelerated triage, supported smarter patch management processes, and aligned detections with adversary TTPs using the MITRE ATT&CK framework.

NOC/SOC INTEGRATED ARCHITECTURE



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