



CASE STUDY:

Global dental and pharmaceutical company enhances detection, reduces exposure, and improves compliance

INDUSTRY: PHARMACEUTICAL

About the client

The client is a multinational leader in the dental and pharmaceutical industries, operating manufacturing and research facilities in over 150 countries. Its portfolio includes medical devices and pharmaceuticals supplied to more than one million customers worldwide.

The client's challenge

As a global provider of dental and pharmaceutical products, the client faced increasing exposure across its manufacturing, research, and digital environments. Rapid expansion of connected systems and a globally distributed workforce had widened the organization's attack surface, making it harder to detect and contain threats before they could impact operations.

Ransomware, intellectual property theft, and supply chain compromise had emerged as critical risks across the healthcare and life sciences sector. With valuable research data and personally identifiable information (PII) under constant threat, the client recognized the need to strengthen its visibility, detection, and response capabilities.

The company also faced rising regulatory pressure to maintain compliance across multiple jurisdictions, including stringent data protection and cybersecurity standards for medical device manufacturers. Fragmented monitoring systems and a reliance on manual processes limited the organization's ability to identify exposures in real time or validate the effectiveness of existing controls.

To address these challenges, the client sought a strategic cybersecurity partner capable of delivering 24x7 managed detection and response, enhanced automation, and a threat-led approach to improve both security operations and regulatory resilience.

Benefits



Improved threat detection and response: The client achieved faster detection and containment of threats across global manufacturing and research sites, reducing mean time to detect and respond through automation, correlation tuning, and use case optimization.



Reduced cyber exposure: Unified visibility across IT, OT, and cloud environments closed critical blind spots and enabled proactive management of vulnerabilities, misconfigurations, and risky assets before they could be exploited.



Stronger compliance and audit readiness: CyberProof's framework supported alignment with data protection and healthcare regulations such as GDPR, HIPAA, and regional medical device cybersecurity standards, reducing regulatory exposure and ensuring operational continuity.



Operational resilience and efficiency: Integration of threat-led automation and continuous exposure management (CTEM) reduced manual workloads for analysts, improved collaboration across SecOps teams, and enhanced the client's ability to sustain long-term cyber resilience.



Our solution

To address the client's growing exposure to cyber risk, CyberProof implemented a comprehensive, threat-led security operations framework designed to deliver proactive detection, faster response, and continuous validation of defenses. The approach integrated advanced automation, contextual threat intelligence, and deep domain expertise across multiple CyberProof delivery centers.

24x7 managed SOC services

CyberProof established a fully managed Security Operations Center (SOC) providing round-the-clock monitoring across the client's global operations. The SOC unified visibility across IT, OT, and cloud environments, detecting early indicators of ransomware, data theft, and insider activity. Leveraging CyberProof's service delivery platform, the client gained a single view of threats, with prioritized alerts based on severity and business impact.

SIEM platform and content management

CyberProof optimized the client's existing SIEM ecosystem by consolidating diverse data sources and migrating core monitoring functions to a cloud-native Microsoft Sentinel deployment. This modernization reduced noise and enhanced correlation accuracy, improving mean time to detect (MTTD) and mean time to respond (MTTR). Automated playbooks were developed for high-frequency alerts, accelerating triage and reducing analyst workload.

Use case management

To ensure detections aligned with real adversary behavior, CyberProof deployed its Use Case Management Service, mapping all content to the MITRE ATT&CK framework. Analysts developed and continuously refined use cases specific to the healthcare and pharmaceutical threat landscape, including data exfiltration, supply chain compromise, and unauthorized access to sensitive IP. Each use case was validated against live telemetry, closing critical visibility gaps and improving operational readiness.

Digital forensics and Incident Response (DFIR)

CyberProof's global DFIR team provided rapid investigation and containment support for incidents across the client's distributed manufacturing and R&D sites. Advanced automation and AI-assisted enrichment enabled faster root-cause analysis and evidence preservation, ensuring compliance with regulatory obligations such as GDPR and HIPAA.

Advanced SOC services and continuous exposure management

CyberProof's exposure management approach combined proactive threat hunting, vulnerability insights, and continuous validation of security controls. Regular exposure assessments identified misconfigurations, risky assets, and unpatched systems — allowing the client to prioritize remediation efforts based on real-world adversary techniques. These insights were integrated into ongoing SOC operations to strengthen resilience and maintain a risk-aligned security posture.

Results

Through its partnership with CyberProof, the client has transitioned to a proactive, threat-led security model that has strengthened both operational resilience and compliance posture. The deployment of a unified, cloud-native SOC improved visibility across global manufacturing and research networks, reducing response times and minimizing exposure windows. Today, the organization operates with greater confidence, supported by continuous exposure management, automated detection and response, and clear alignment between cybersecurity operations and business risk.

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