CyberProof®
A UST Company

Better Security,
Together.

CASE STUDY:

Leading UK retail and healthcare chain enhances threat detection and vulnerability management through Continuous Threat Exposure Management

INDUSTRY: RETAIL & HEALTHCARE

About the client

Our client is a major UK-based retail and healthcare chain with tens of thousands of employees. Operating in a highly regulated and complex sector, the organization faced mounting pressure from targeted threat actors and needed to ensure strong detection capabilities across its enterprise.

In this environment, they partnered with CyberProof to assess and strengthen their security posture by identifying detection gaps and prioritizing real-world threat risks—particularly from advanced persistent threats (APTs).

Client challenge

Operating in a threat-rich landscape, the client sought a clearer understanding of their exposure to targeted threat actors, including Turla, a known nation-state adversary. Goals for the security posture assessment included:

- Conducting a comprehensive security posture assessment across their enterprise.
- Evaluating detection coverage against high-priority MITRE ATT&CK techniques.
- Identifying exposure to exploitable vulnerabilities (CVEs) used by threat actors.
- Correlating these findings with actual threat actor tactics, techniques, and procedures (TTPs) to inform prioritization.

The complexity of their infrastructure and the breadth of threats they faced required a highly customized, threat-informed approach.

After evaluating MDR providers, CyberProof stood out by demonstrating how a Microsoft Sentinel-based

architecture could reduce long-term costs and improve operational efficiency.

CyberProof had a consultative approach, technical alignment, and scalable commercial model which positioned the vendor as the trusted partner of choice.

Key Benefits

- **Clear visibility of detection gaps**
  The assessment surfaced multiple high-priority MITRE techniques that had insufficient or no detection coverage.
- **Threat-aligned detection engineering** The findings created a roadmap for prioritized tuning and development of detection content tailored to high-risk adversaries like Turla.
- **Strategic risk reduction from known CVEs**
  A critical CVE associated with Turla was identified on a small number of assets, and another was found across a broad footprint—prompting prioritized remediation.
- **Smarter vulnerability management**
  The client shifted from a CVEs-only model, where they only defended against generic threats, to a threat-informed risk approach, improving triage based on real-world exploitability.

Our solution

CyberProof executed a comprehensive Continuous Threat Exposure Management (CTEM) assessment and service delivery designed to give the client a practical, intelligence-led view of their detection and vulnerability landscape. This was carried out through a structured, four-phase process that blended technical analysis with threat actor intelligence and MITRE ATT&CK alignment:

Threat Modeling

The engagement began with the creation of a tailored threat profile based on the client's industry, operational environment, and known targeting by APTs. Special emphasis was placed on threat actors relevant to the retail and pharmaceutical sectors, particularly Turla, a sophisticated, nation-state-aligned adversary known for targeting large enterprises.

Data Ingestion and Inventory Analysis

CyberProof ingested critical datasets including asset inventory, existing detection configurations, and current vulnerability records. This phase laid the groundwork for correlating what assets were present, how they were defended, and where exploitable exposures existed.

Detection Capability Mapping

All existing detection rules and security tooling were evaluated and mapped against the MITRE ATT&CK framework. This revealed concrete visibility gaps — specifically in several high-priority ATT&CK techniques that Turla and similar actors are known to exploit. The results gave the client actionable insights into which techniques were under-covered or entirely blind.

Threat Actor TTP Correlation

Finally, the team overlaid known TTPs used by high-priority adversaries like Turla against the detection and vulnerability data. This analysis was powered by CyberProof's CTEM platform and shared with other teams working within the client's environment to enhance coverage across existing systems. This allowed CyberProof to contextualize vulnerabilities not just by severity (e.g., CVSS score), but by how likely they were to be exploited in a real attack scenario — delivering practical, risk-informed prioritization guidance.

This entire process enabled a strategic pivot: from general security hygiene to threat-informed defense. Instead of relying solely on static scoring systems, the client could now focus detection engineering and vulnerability remediation where it would reduce the most real-world risk.

These insights now serve as a blueprint for advancing the client's detection capabilities, ensuring future investments are tightly aligned with their most pressing threat exposures.

CyberProof®
A UST Company

Better Security,
Together.

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

© 2025 CyberProof Inc. All Rights Reserved.