CYWARE™ | Case Study

Global Consumer Healthcare Leader Transforms Threat Intelligence and Incident Response with Cyware

A global leader in consumer healthcare supports millions of consumers worldwide through a complex, distributed digital environment, which presented a significant scale and complexity challenge in its cybersecurity operations.To maintain its commitment to consumer safety and data integrity, the organization manages a sophisticated Security Operations Center (SOC) tasked with defending a massive global footprint of identity and device assets.

Transitioning to a Proactive Defense Posture

By integrating enriched identity and device context directly into security workflows, the organization eliminated manual data retrieval and transformed a reactive posture into an automated, proactive defense.

Overview

The following table outlines the critical visibility and operational gaps identified by the security team and how Cyware's integrated platform addressed each challenge to drive improved business outcomes.

	Cyware Solution	*Business Outcome*
Slow Investigation Manual data retrieval delayed incident response.	**Cyware Orchestrate** Automated investigation and tool integration.	**Automation** Manual tasks replaced by automated data pulls.
Alert Fatigue Low-context alerts overwhelmed analyst capacity.	**Integrated Orchestration** Cohesive orchestration across the SOC.	**Consistency** Unified stack ensures consistent response quality.
Visibility Gap Disconnected identity, device, and log data.	**Cyware Respond** Unified case management and incident tracking.	**Efficiency** Structured context accelerates informed decision-making.

> By partnering with Cyware, we have moved from manually hunting for context to a model where enriched intelligence is delivered directly to our analysts. This collaboration hasn't just improved our tools; it has fundamentally strengthened our defence posture
>
> *— Lead Security Operations Engineer*

Driving Operational Excellence through Automated Threat Intelligence

> **Streamlined Workflows:** Moved from a fragmented process to a streamlined one by pulling enriched context directly into investigations.

> **Reduced Analyst Toil:** Replaced manual data retrieval with pre-built integrations to minimize manual intervention.

> **Optimized Response:** Achieved faster investigations through structured context and a more interconnected security stack.

Solving Critical Investigation Bottlenecks and Visibility Gaps

The organization faced rising alert fatigue and critical gaps in visibility. Analysts lacked sufficient data points, forcing a reactive posture that stretched investigation timelines across a distributed environment. By deploying Cyware, the team addressed inadequate context generation to empower faster, more informed decision-making.

How Integrated Intelligence Drives Investigation Velocity

The implementation focused on pulling enriched, relevant context directly into the investigation workflow. By utilizing mock databases to simulate production data, the team successfully proved out automation of manual investigation steps through deep integration with the following security systems: Three integrations were brought live during the POC.

Splunk
Automated queries pulling user and device logs mapped to MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs).

Active Directory
On-demand pull of user identity and account information directly into the investigation case.

ServiceNow CMDB
Device context and configuration data surfaced automatically during incident triage.

> Cyware provides more than just a toolset; it's a collaborative partnership. The ability to co-develop connector capabilities and see them productized has given us immense confidence in the scalability of our incident management workflows.
>
> — *Senior Director*

Impact of Automation and Unified Intelligence

To address these visibility gaps, Cyware executed a "Run Deep, Not Wide" implementation focused on surgical precision. This 30-day strategy targeted high-value use cases to prove platform strengths within the client's actual environment. By co-designing custom workflows and specialized Cyware Respond tracking fields, we established a refined operational baseline tailored to the global security team's specific reporting requirements.

Investigation Velocity: Transitioned from manual context hunting to automated triage in minutes.

Contextual Enrichment: 100% of cases now trigger with identity (AD) and device (CMDB) data pre-populated.

Analyst Efficiency: Estimated saving of significant analyst hours per month by automating data retrieval.

What Sets Cyware Apart

Beyond the technical capabilities, the client's team pointed to the quality of the working relationship with Cyware as a defining factor. The engagement was collaborative at every stage, from scoping the POC use cases to working through implementation details on the integrations.

The co-development model that emerged from this engagement is a direct reflection of how Cyware approaches customer partnerships. The client's security engineers are not just end users of the platform. They are active contributors to making it better, and Cyware invests in those contributions by productizing them for the benefit of the entire customer community.

About Cyware

Cyware is leading the industry in Agentic-powered Operational Threat Intelligence and Collective Defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, with orchestration and automation, eliminating silos and enabling organizations to outmaneuver adversaries faster and more effectively. From enterprises to government agencies and ISACs, Cyware empowers defenders to turn intelligence into impact.

Learn More