CYWARE™

CASE STUDY

Global Food and Beverages Leader Makes Security More Palatable with Cyber Fusion

OVERVIEW

A multinational food, snacks, and beverage manufacturer, was utilizing a legacy Security Orchestration, Automation, and Response (SOAR) platform for case management and security automation. However, the incumbent solution was failing to meet their requirements forcing them to find a more capable solution.

CHALLENGES

The client was encountering numerous challenges that were impacting their operational efficiency, including:

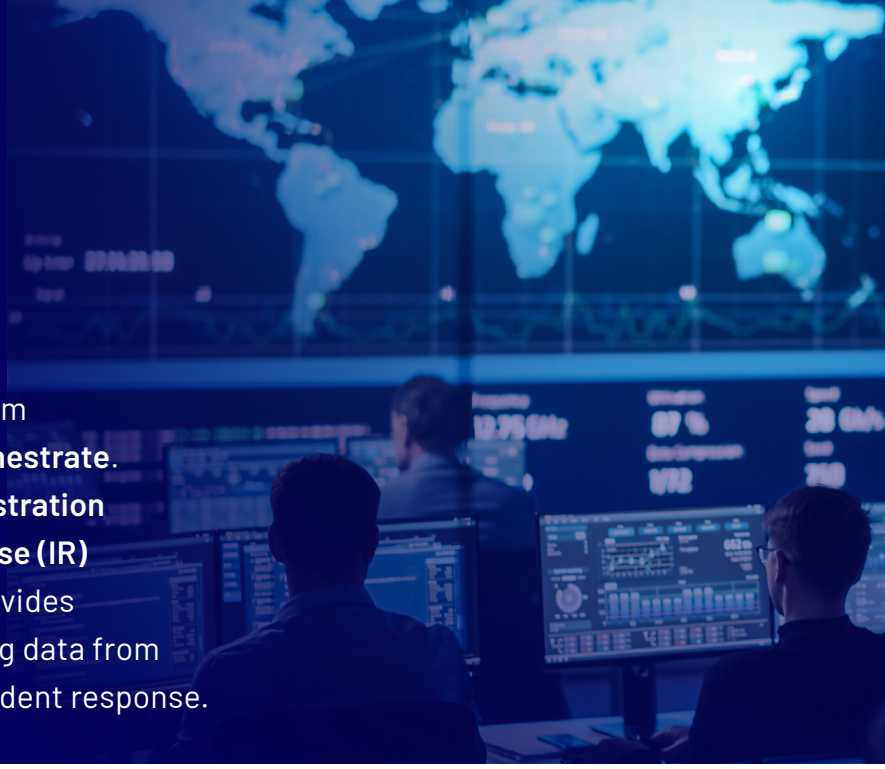
1. **Limited Case Management Capabilities**
   The legacy SOAR solution had basic case management capabilities, which restricted streamlined incident tracking and resolution.

2. **Lack of Real-Time Incident Onboarding**
   Incident onboarding from the SIEM and log management tool could only run periodically, not in real time, leading to delays in incident response.

3. **Complex Playbook Lifecycle Management**
   Making changes to workflows was a daunting task due to the close coupling of the orchestration/automation and case management systems.

4. **Poor Reporting and Dashboard Capabilities**
   The client was reliant on their Security Information and Event Management (SIEM) system for reporting due to the incumbent product's inadequate dashboard and reporting capabilities.

SOLUTION: CYBER FUSION

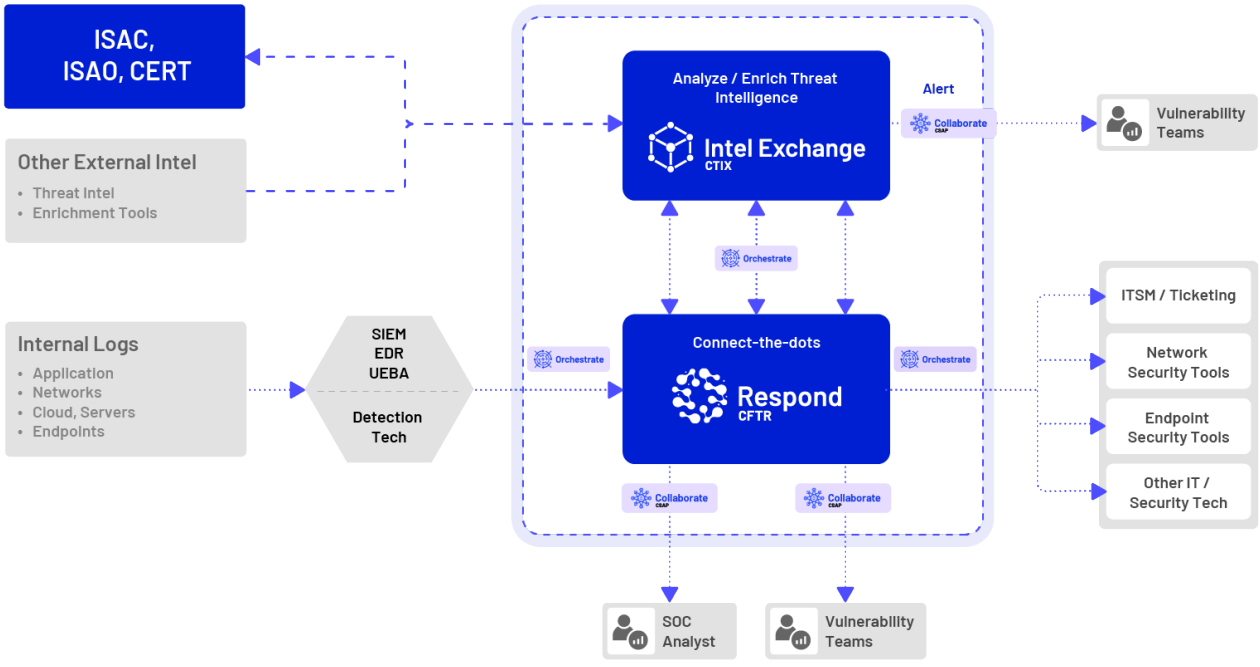


Cyware's Cyber Fusion Center was deployed in a phased manner. Initially, we deployed our advanced Case Management and Threat Response solution, **Respond (CFTR),** in tandem with our security orchestration solution, **Orchestrate**. Cyware, uniquely **de-couples Security Orchestration and Automation (SOA) from Incident Response (IR) and Case Management**. This architecture provides greater flexibility with Orchestrate connecting data from any source, and driving action far beyond incident response.

After the SOAR components were deployed, the client also integrated **Intel Exchange (CTIX),** Cyware's flagship **threat intelligence platform (TIP)** to drive full threat **visibility** through centralized and automated threat data aggregation, analysis, and actioning. With Respond, Orchestrate, and Intel Exchange, the client was fully transitioned to a CFC.

Cyware also leveraged its automated playbook migration engine to transition all existing client use cases from the incumbent SOAR solution to Cyware's CFC within a record time which ensured that the client was able to maintain critical security operations without disruption while enhancing their overall cyber defense efficacy and threat handling capability.

Cyber Fusion Center Architecture



The complete Cyber Fusion solution had all the capabilities to address the client's challenges and deliver a robust, flexible, and real-time responsive threat response and security automation system tailored to their unique needs.

A quick overview of Cyware CFC capabilities deployed in the client's infrastructure:

Respond
CFTR

An automated incident analysis and threat response platform informed by extensive data visibility and advanced correlation to drive intelligent action from security teams.

Orchestrate

A vendor-agnostic, low-code/no-code orchestration and automation platform for connecting and integrating Cyber, IT, and DevOps workflows across the cloud, on-premise, and hybrid environments.

Intel Exchange
CTIX

An automated Threat Intelligence Platform (TIP) for ingestion, enrichment, analysis, prioritization, actioning, and bidirectional sharing of threat data.

USE CASES SOLVED

The Cyber Fusion solution seamlessly integrated with the client's extensive SOC infrastructure. This deployment effectively solved various use cases by orchestrating data and actions across all security and IT tools. The full solution includes:

- **Incident Onboarding**
  Enabling real-time onboarding of incidents from the SIEM and log management tools, reducing delay and improving response times.
- **Incident Handling**
  Robust case management provides customizable incident workflow building, allowing for more efficient and personalized incident handling.
- **Threat Intel Enrichment and Analysis**
  The TIP platform enables automated enrichment of data from prominent enrichment databases, commercial providers, and internal security and IT tools.
- **Custom Playbooks**
  The client was able to build custom playbooks for automating response to botnets, phishing attacks, brand impersonation, etc.
- **Threat Actioning**
  The client also built custom threat management and actioning workflows for incidents, malware, and vulnerabilities, detected in their IT and OT systems.

All use cases are fully automated.

OUTCOME AND BENEFITS

The implementation of Cyber Fusion significantly enhanced the client's security posture. Key benefits included:

- **Independent Automation Capabilities**
  The flexible design of the solution enables the client to build independent automation workflows, without having to route every automation workflow through case management.
- **Customized Incident Handling**
  Customizable case management provides efficient and tailored incident handling. In addition, the client can now manage cases for malware, vulnerabilities, threat actors, and assets.
- **Complete Threat Visibility**
  The native integration of TIP capabilities and connecting the dots capability of Cyber Fusion provides the client with a comprehensive and real-time view of the threat landscape. This increased visibility allowed for faster and more accurate responses to potential threats.
- **Reduced Mean Time to Respond (MTTR)**
  Real-time incident creation, as opposed to the previous periodical delays, led to a considerable reduction in MTTR .
- **Improved Decision-Making**
  Advanced analytics and reporting capabilities provided detailed threat insights and predictive capabilities. This allows the client's security team to make more informed, data-driven decisions.
- **Proactive Threat Management**
  The intelligence capabilities of the platform enables proactive threat hunting and management. The client can now preempt potential threats and take preventive measures, reducing their risk exposure and bolstering their cybersecurity resilience.
- **GDPR and Data Privacy Compliance**
  The SaaS solution is hosted within the EU region, meeting the client's requirements for GDPR and data privacy compliance.

For more information you can reach us at :

Cyware

111 Town Square Place Suite 1203 #4,
Jersey City, NJ 07310
sales@cyware.com | www.cyware.com

CYWARE™