CYWARE™

CASE STUDY

# Global Elevator Leader Takes Security to the Next Level

## OVERVIEW

A global leader in the elevators, escalators, and vertical transportation systems was using a legacy threat intelligence platform (TIP) to manage its security needs. The organization was also relying on the legacy TIP's basic case management feature to manage incidents. The legacy TIP fell short in meeting the requirements of its internal teams - product security incident response team (PSIRT), security operations center (SOC), and threat intelligence (TI) teams. They were on the lookout for a comprehensive solution, aiming to automate all threat intelligence operations and facilitate seamless case management and threat response automation.

## CHALLENGES

### 1 Inadequate TIP Capabilities

Absence of an advanced TIP led to gaps in threat intelligence operations, affecting detection, hunting, vulnerability assessment, and response actions.

### 2 Basic Case Management

Lack of an advanced case management platform resulted in inefficient incident response processes, thus exacerbating the complexity of issues and increasing resolution time.

### 3 Poor Threat Analysis and Visibility

Without centralized threat correlation and investigation, there was limited threat visibility, causing ineffective response prioritization.

### 4 Manual Security Operations

Limited automation and orchestration capability resulted in manual security workflows resulting in inefficient processes, operational challenges, and high MTTR.

# SOLUTION: CYBER FUSION

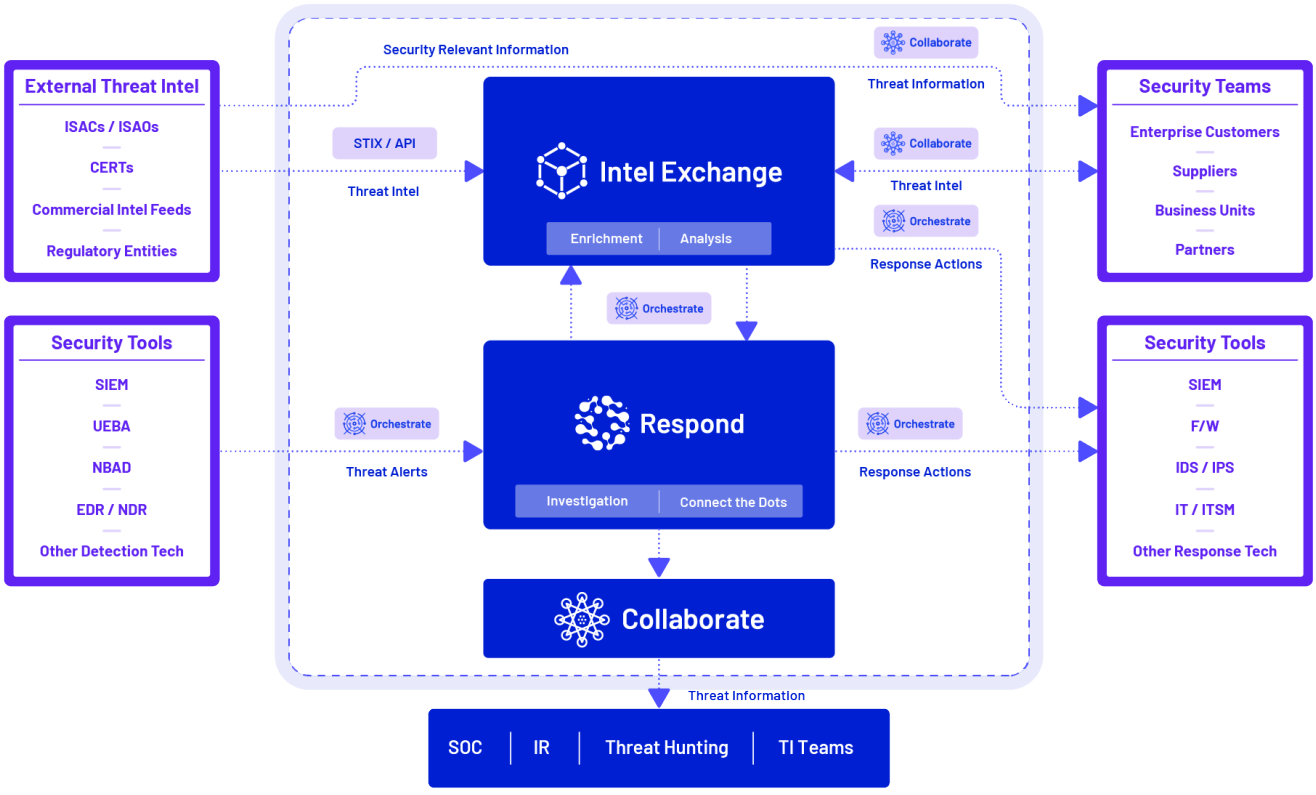
Cyware's Cyber Fusion suite of solutions including Intel Exchange, Respond, and Orchestrate platforms were deployed in the organizations SOC to automate security operations while enabling a seamless flow of actionable threat intelligence into threat detection, threat hunting, vulnerability management, and incident response operations.

**Intel Exchange** is an automated threat intelligence platform (TIP) designed for ingestion, enrichment, analysis, prioritization, actioning, and bidirectional sharing of threat data. Deployed as a replacement to a legacy TIP, this platform enables the manufacturer to ingest, enrich, and analyze threat intelligence from its monitoring tools, external feeds, enrichment sources, and email gateways, and share it with its security teams.

**Respond** is an automated incident analysis and threat response platform that helps automate and streamline incident response processes, enabling quick and efficient threat response with a reduced workload on security teams. It provides centralized case management for incidents, malware, vulnerabilities, and threat actors, while connecting the dots for full threat visibility and proactive response.

**Orchestrate** is a vendor-neutral, low-code orchestration and automation platform that serves as a connecting fiber between all the cybersecurity and IT tools deployed in the organization's SOC. The platform eliminates manual efforts needed in orchestrating data and triggering automated actions across the detection and monitoring tools, Intel Exchange, and Respond platforms.

## Cyber Fusion Center in Action



# USE CASES SOLVED

Cyware implemented several use cases for the manufacturer, enabling them to optimize their cybersecurity operations, fortify their defenses, and bolster security efficiency. All use cases are fully automated. The key use cases included:

1. **Threat Intelligence Management**
   Automated multiple stages of the threat intelligence lifecycle, including ingestion, enrichment, and analysis, allowing security teams to ingest, enrich, and correlate IOCs from various intel sources and eliminate false positives to add context to the threat data.

2. **Threat Bulletins and Reports Delivery**
   Automatically published threat bulletins and reports with their PSIRT, TI, and SOC teams, equipping them with contextualized and rich threat intel required for investigations.

3. **Incident Onboarding**
   Automated onboarding and case creation of incidents, malware and vulnerabilities directly from SIEM, EDR, and emails for further threat investigations, triaging, and analysis.

4. **Incident Analysis and Management**
   Real-time incident analysis involving threat indicator enrichment, retrospective search using time-based tags to analyze and retrieve historical intelligence, and connecting the dots between assets, malware, vulnerabilities, threat actors, and incidents for proactive threat analysis and response.

5. **S-BOM Software Composition Analysis**
   Assessed and managed the components and dependencies in software applications, providing insights into potential security vulnerabilities.

6. **Threat Actioning**
   Automated blocking of malicious IOCs on security solutions like Firewall and EDR, updating SIEM Watchlist to enhance threat detection and response capabilities. This use case also involved automated blocking of malicious emails to prevent any further communication from that address.

# BENEFITS AND OUTCOMES

With Cyware, the manufacturer can handle huge volumes of IOCs without compromising the performance of their security operations with multiple benefits:

- **Highly Efficient Security Operations**
  Automating various security processes, such as threat intelligence enrichment, correlation, incident onboarding and analysis, and threat actioning significantly reduces the reliance on manual efforts, resulting in accurate threat analysis and response.

- **Large IOC Volume Handling**
  By efficiently ingesting, analyzing, and actioning large volumes of structured and unstructured threat data (IOC), the customer is able to scale threat intelligence operations ensuring comprehensive threat analysis and visibility.

- **Actionable Threat Intelligence**
  By enriching threat data with relevant context from multiple intelligence sources, the customer receives actionable insights empowering them to make well-informed decisions during investigations.

- **Proactive Threat Mitigation**
  By automating multiple stages of the threat intelligence and response lifecycle, the customer is able to proactively detect and respond to potential security threats before they could escalate into incidents.

- **Reduced MTTR**
  Automated incident onboarding and closure enables different internal security teams to respond swiftly to security incidents, minimizing the time between detection and resolution.

- **Inter-Team Collaboration**
  Centralized threat management and integrated threat intelligence operations facilitate seamless collaboration among all security teams, fostering a unified approach to security challenges and enhancing the organization's overall defense strategy.

- **Enhanced Threat Hunting and Detection**
  Connecting the dots, retrospective search capabilities, and integrated threat intelligence operations enable the customer to conduct historical data analysis, identify hidden patterns, and detect new threats thereby fostering threat hunting and detection operations.

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™