CYWARE™ | TEAM CYMRU | Solution Brief

Threat Intel Operationalization for Accelerated Defense

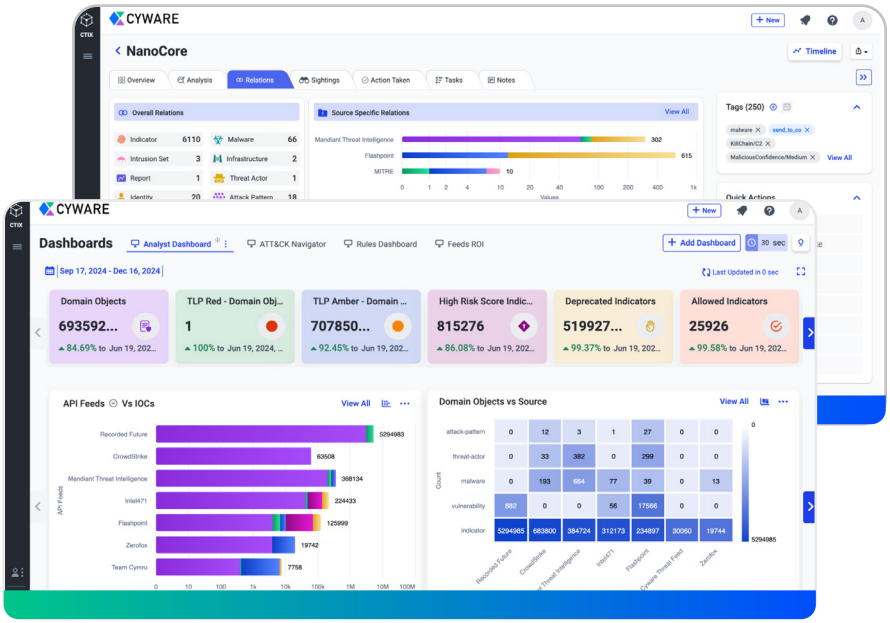
Cyware Intel Exchange now with Team Cymru

Organizations face challenges in gaining timely visibility into malicious infrastructure like C2 servers, botnets, and phishing campaigns. Manual threat intelligence processes hinder efficiency, while the overwhelming signal-to-noise ratio complicates threat prioritization.

Solution

Cyware Intel Exchange platform now addresses these gaps by integrating with Team Cymru's high-fidelity threat intelligence feeds to deliver actionable insights and enriched data. By leveraging Team Cymru's visibility into malicious activities, the integration enables operationalization of enriched intelligence for quicker decision-making and better prioritization of threats.

Intel Exchange correlates these feeds with internal data, helping organizations detect, investigate, and respond to cyber threats more effectively. It also allows security teams to visualize relationships between threat objects, improving their understanding of attack patterns and shared risks. This integrated solution unlocks accelerated time-to-action, situational awareness of malicious activity, and streamlined threat intel vendor management.



Key Capabilities

- Seamless ingestion of Team Cymru's threat intelligence feeds into Cyware Intel Exchange platform.
- Automated normalization, correlation, and analysis of threat data to streamline intelligence workflows.
- Enhanced ability to track adversary infrastructure, monitor malware family activity, and correlate attack patterns with enriched threat data.
- Advanced threat prioritization with Cyware's scoring and tagging capabilities to focus on actionable risks.
- Generate custom threat reports and bulletins, and map MITRE ATT&CK TTPs for advanced analysis.

CYWARE™

Cyware and Team Cymru Integration Use Cases for Threat Intelligence Teams

IP-Based Threat Detection & Hunting

Employ precise IP intelligence to uncover and address malicious activities, including botnets, C2 servers, and compromised devices. This supports efforts to mitigate vulnerabilities by identifying harmful IPs scanning networks or communicating with malware.

Phishing Campaign Identification

Detect and neutralize phishing campaigns by analyzing indicators tied to spoofed domains and other tactics. Organizations can use this data to block phishing threats before they compromise user accounts or sensitive information.

Adversary & Malware Campaign Analysis

Understand adversary behavior and campaign infrastructure through detailed monitoring of malware families and attack attributes. Visualize relationships between different threats, helping identify interconnected attack patterns. This enables timely responses to evolving threats and effective disruption of malicious operations.

IOC Enrichment

Add depth to threat intelligence with enriched context about IOCs, such as geographical origin and associated malicious activities. This fosters a more comprehensive understanding of threats and streamlines incident response workflows.

Cyware Intel Exchange

Cyware Intel Exchange is an advanced Threat Intelligence Platform (TIP) designed to centralize, enrich, and rapidly operationalize threat intelligence. It provides robust automation, seamless integrations, and advanced analytics, empowering organizations to effectively manage their threat intelligence workflows and improve collaboration across teams.

Team Cymru BARS and Controller Feeds

The integration allows security teams to leverage Team Cymru's BARS (Behavioral Analysis and Reporting System) feed, monitoring over 50 billion flow records daily to detect malicious trends, and the Controller feed, which tracks over 150,000 command-and-control (C2) servers worldwide. These feeds provide actionable insights into malicious domains, IPs, and infrastructure, enabling organizations to counter cyber threats effectively.

For more information:

111 Town Square Palace Suite 1203 #4
Jersey City, NJ 07310

cyware.com | government@cyware.com

CYWARE™