CYWARE™ | Datasheet

Cyware Intel Exchange

Transform Threat Intelligence Into Intelligent Action

Cyware Intel Exchange is a fully automated Threat Intelligence Platform (TIP) that ingests, enriches, prioritizes, and operationalizes threat intelligence at scale. Powered by agentic AI and built-in automation, Cyware Intel Exchange reduces the noise of raw data and transforms it into high-fidelity insights for faster, smarter action. Whether you're launching a new threat intel program or scaling up your threat intelligence operations, Cyware Intel Exchange adapts to your maturity level.

Cyware Intel Exchange helps security teams automate the entire threat intelligence lifecycle, contextualize threat analysis, take proactive action, and share threat intelligence bi-directionally. With its modular, scalable architecture and built-in integrations for ingestion, enrichment, and actioning, security teams can stop stitching tools together and start operationalizing threat intel rapidly.

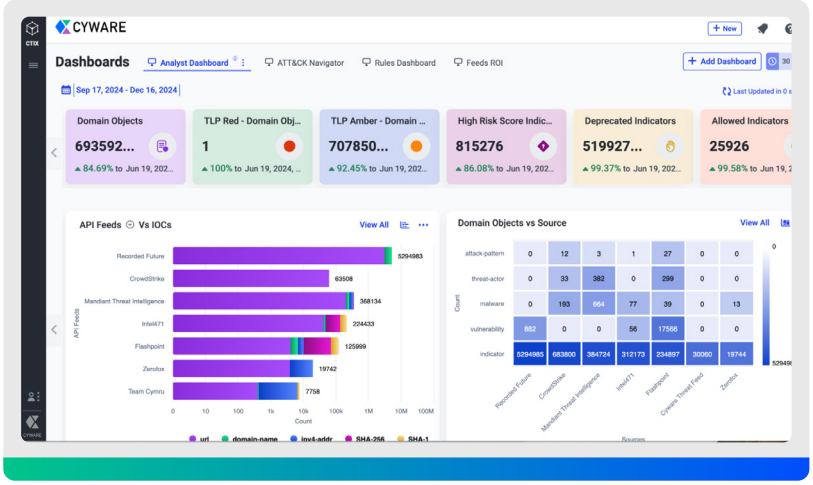

Fig 1. *Cyware Intel Exchange Dashboard*

The Key to Unified Threat Intelligence Management

AI-Powered Threat Intelligence Parser
Automatically extracts IOCs, TTPs, threat actors, malware, vulnerabilities, and courses of action from text, documents, or websites, eliminating manual entry. Seamlessly integrated with the Quick Add Intel module.

AI Threat Intel Summarization
Generates concise, context-rich summaries of threat reports and related objects, helping analysts cut through noise and respond faster. Integrated within Threat Object details.

AI-Powered Threat Intel Crawler (Browser Plugin)
Instantly converts threat intelligence from websites into structured, enriched data. Eliminates manual scraping, reduces human error, and speeds up data ingestion for fast, reliable threat data capture.

Cyware MCP Server Integration
Enables secure, seamless communication and orchestration across AI agents, Cyware products, and external systems, powering real-time collaboration and autonomous workflows.

Automated Ingestion & Normalization
Ingest, deduplicate, and standardize threat data into the STIX format automatically from OSINT, commercial feeds, internal tools, and community sources.

Flexible Enrichment & Advanced Correlation
Automatically enrich indicators using built-in enrichment connectors and correlate with historical intel.

CYWARE™

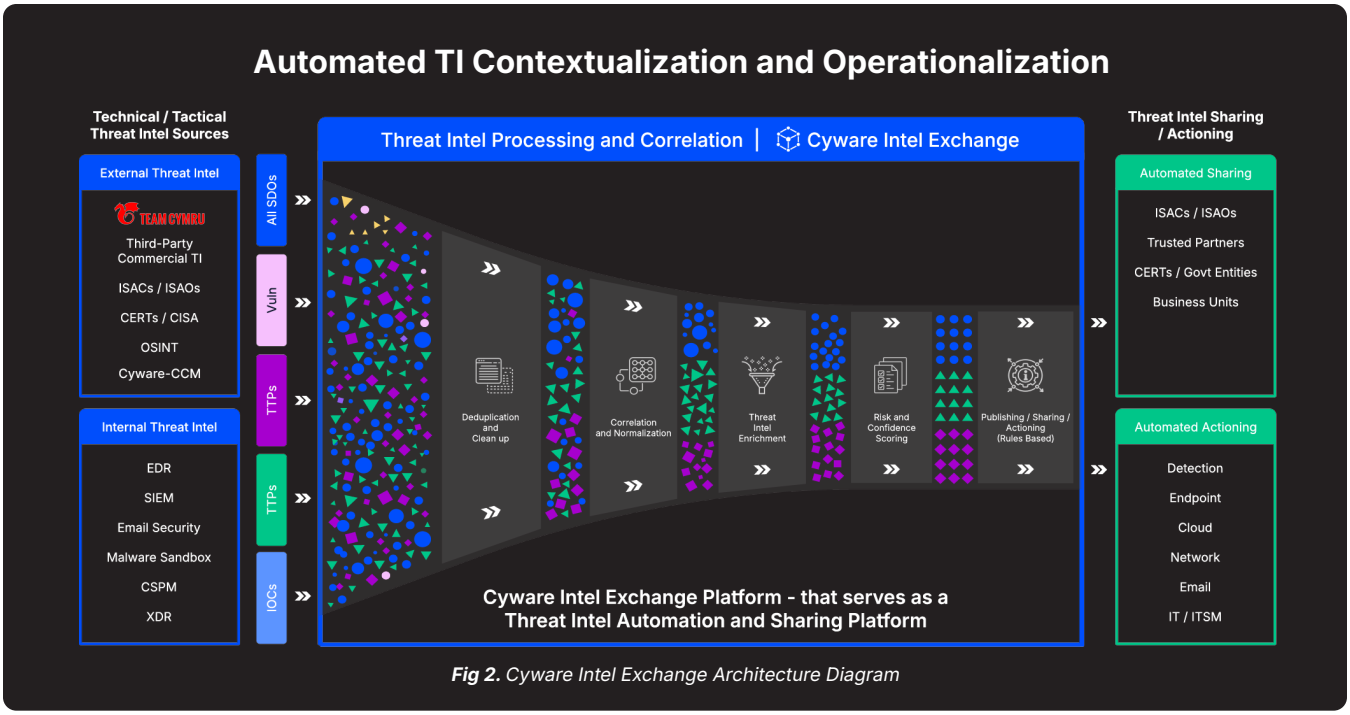

Fig 2. *Cyware Intel Exchange Architecture Diagram*

Why Intel Exchange Stands Apart

Multi-Source Threat Intel Operationalization

- Format-agnostic ingestion from STIX, MISP, JSON, CSV, email, and more
- Automated collection from OSINT, commercial feeds, ISACs, CERTs, and internal tools
- Automated de-duplication and normalization to eliminate noise and false positives

Visual Threat Analysis & Hunting

- Visual investigation canvas with multi-dimensional threat mapping
- Built-in MITRE ATT&CK Navigator and sandbox detonation capabilities
- Cyware Query Language (CQL) for complex intel searches

AI-Augmented Enrichment & Prioritization

- Automatically extracts and summarizes IOCs, TTPs, malware, vulnerabilities, threat actors, and recommended actions from any text, document, or report.
- Eliminates manual data entry, reduces human error, and helps analysts quickly digest complex intelligence.
- Speeds up threat analysis, reduces alert fatigue, and accelerates decision-making and response times.

Automated Intel Actioning & Dissemination

- Automation rules for threat intel management tasks and response actions
- STIX/TAXII-based bidirectional intel sharing with granular access controls
- Personalized intel reporting and custom dashboards ready for SOC use

AI-Powered Browser Extension

- Turns website-based intel into structured, enriched data in real time
- No manual scraping required
- Compatible with Chrome and Edge; hosted on AWS

Extending Threat Intel Operationalization Through the Cyware Ecosystem

Orchestrate

Drive AI-powered threat intel operationalization and orchestrate security workflows across the cloud and on-premise using Cyware Orchestrate.

Collaborate

Enable secure collaboration and bidirectional intel sharing across trust boundaries for collective defense using Cyware Collaborate.

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation security orchestration and automation solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Cyber Fusion solutions enable secure collaboration, information sharing, and enhanced threat visibility for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAO/CERTs and others) of all sizes and needs.

cyware.com

sales@cyware.com

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