

# 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 advanced AI and built-in automation, 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 an advanced cyber fusion center, 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.

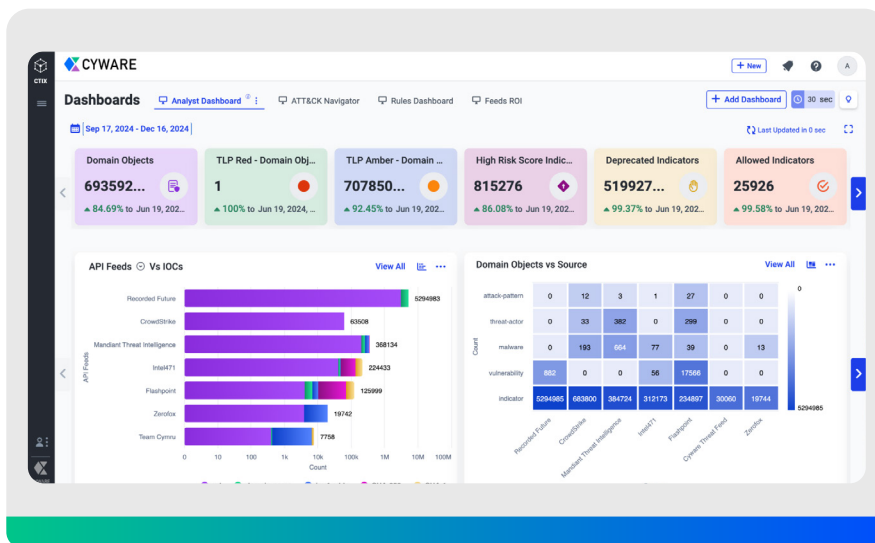


Fig 1. Cyware Intel Exchange Dashboard

## The Key to Unified Threat Intelligence Management

### 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.

### Custom Threat Prioritization

Customizable confidence scoring and tagging to surface threats that matter the most.

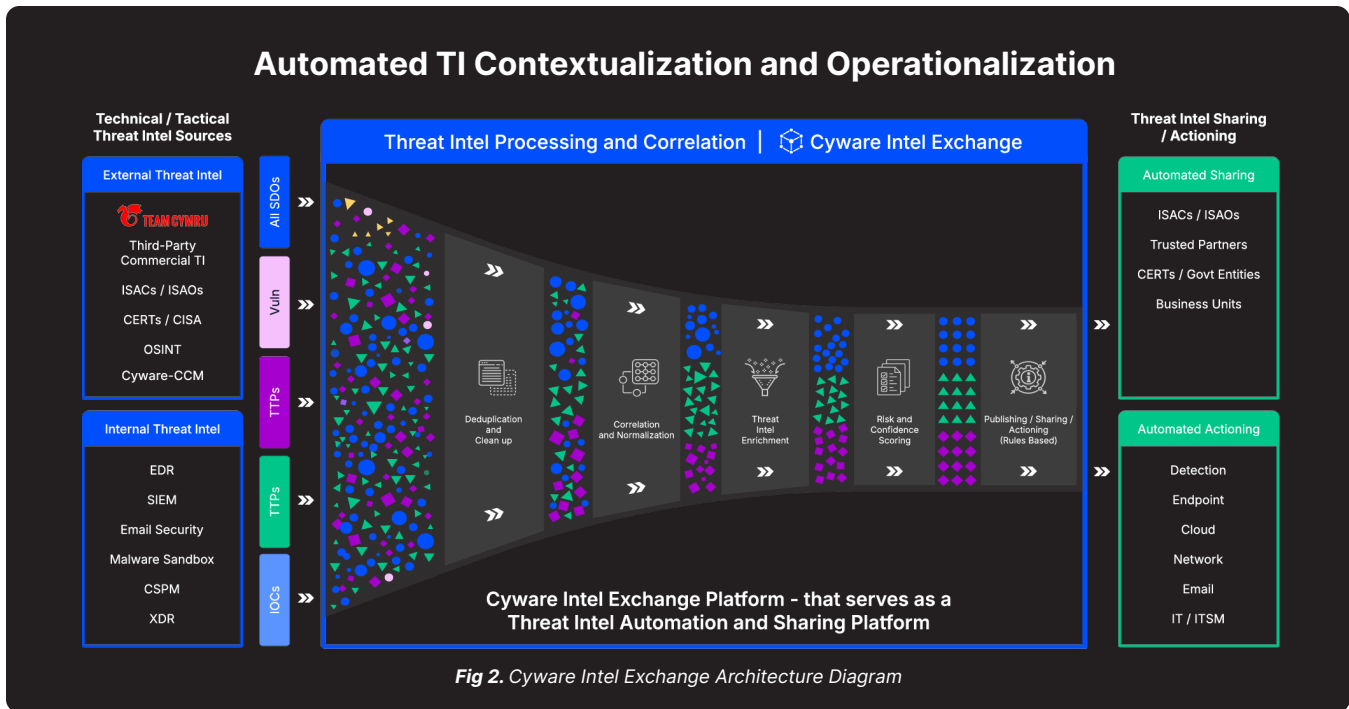
### Visual Threat Investigations

Map threat actor TTPs using the ATT&CK framework and leverage a visual threat investigation canvas to uncover hidden threats.

### Rule-based Automation

Update false positives, block malicious indicators, trigger response playbooks, and more using the built-in rule engine.

## Automated TI Contextualization and Operationalization



### 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

- Integrated enrichment from VirusTotal, Shodan, Polyswarm, and more
- Flexible enrichment policies and correlation with historical intel
- Custom risk scoring based on source credibility, indicator attributes, and enrichment

#### 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

### Extending Threat Intel Operationalization Through the Cyware Ecosystem



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



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](https://cyware.com)

[sales@cyware.com](mailto:sales@cyware.com)

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