CYWARE™

Intel Exchange CTIX

Intel Exchange (CTIX)

A Connected Threat Intelligence Platform (TIP) for Any-to-Any Feed Orchestration, Analysis, and Sharing.

The inability to ingest, analyze, and operationalize threat intelligence has rendered organizations vulnerable to advanced security threats.

Organizations are lacking high-confidence, actionable threat intelligence, which holds the key to identifying, prioritizing, and containing threats targeting their networks and endpoints. The huge amount of threat data shared by internal and external sources ends up overwhelming security analysts, severely impacting threat detection, investigations, and response activities. To overcome these challenges, many organizations are now moving towards automated, connected Threat Intelligence Platforms (TIPs) that single-handedly solve the threat intel lifecycle management needs of security teams.

Intel Exchange (CTIX) is a fully automated connected TIP that leverages AI and ML to automatically ingest, analyze, correlate and take action upon the threat data ingested from multiple external sources and internally deployed security tools in a format-agnostic manner. Intel Exchange's unique capability to ingest and act upon threat data collected from internally deployed security tools is complemented by its client-server exchange-based "Hub and Spoke" design architecture that enables security teams to build trusted sharing communities with their ISACs/ISAOs, CERTs, business units, clients, vendors, peers, and regulatory bodies for exchange of specific, relevant and validated cyber threat intelligence.

Fully Integrated with Premium Feeds, Enrichments, and Security Technologies

- ☑ **Premium and OSINT Threat Feeds** (STIX and API Integrations)
- ☑ **Enrichment Tools** (VirusTotal, Hybrid Analysis, PolySwarm, alphaMountain, etc.)
- ☑ **Security Technologies** - SIEM, SOAR, EDR, F/W, UEBA, IDS/IPS, etc.

INTEL EXCHANGE CAPABILITIES

Multi-source Threat Intel Ingestion

- Internal and External Intel Ingestion (STIX 2.x Compliant)
- Format-Agnostic IOC Conversion & Sharing
- Structured and Unstructured Intel Ingestion
- Full Subscriber and Collection Management

Enrichment, Correlation, and Analysis

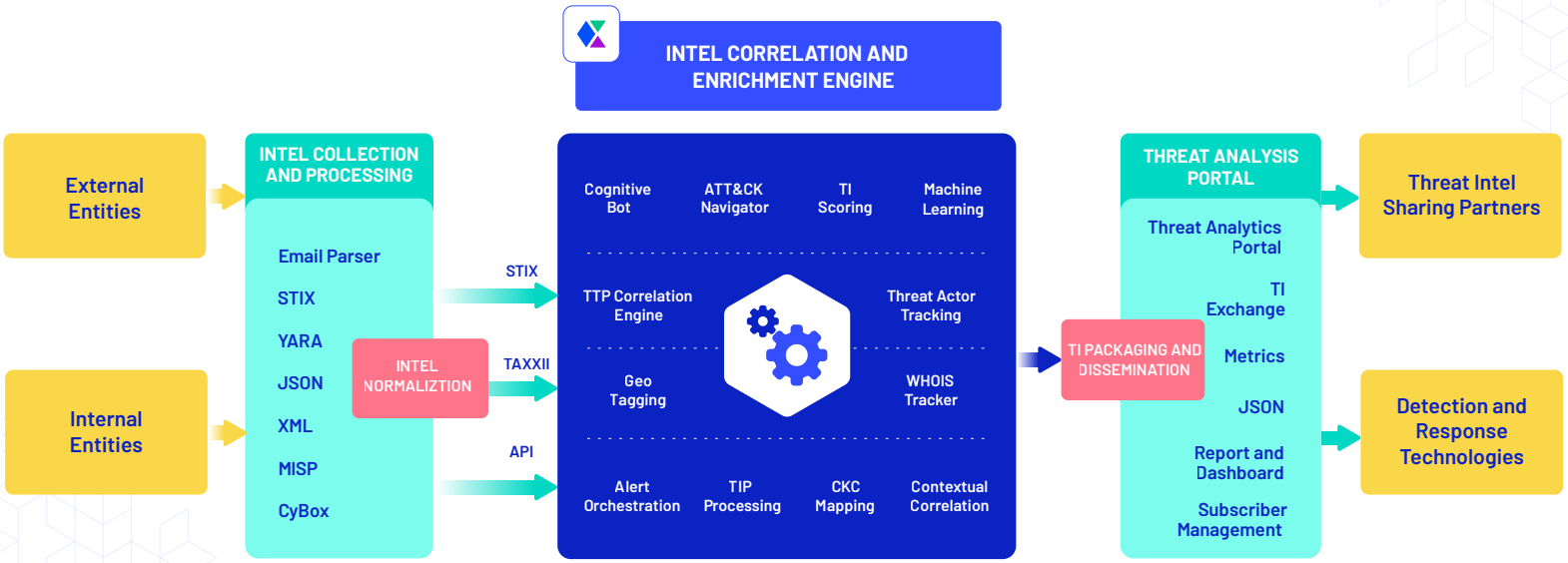
- Enrichment Management and Policy
- IOC Confidence Scoring
- Advanced Rules Engine
- Machine Learning-based Analysis
- Threat Investigations and Visualizations

Threat Intel Dissemination and Actioning

- Hub and Spoke-based Sharing for ISACs/ISAOs, Large Enterprises, etc.
- Internal Sharing with SOC/IR/TI Teams, CISO, etc.
- Intel Actioning in SIEMs, EDRs, Firewalls, IDS/IPS, etc.

All processes and workflows are automated

MICROSERVICES-BASED MODULAR AND SCALABLE ARCHITECTURE



FULLY AUTOMATED THREAT INTEL LIFECYCLE MANAGEMENT

Multi-source Intel Collection

- Ingest threat intel from external sources including TI providers, ISACs/ISAOs, CERTs, peers, etc., and internally deployed security stack including SIEM, UEBA, Firewall, etc.
- Automatically ingest, normalize, and extract threat indicators (IOCs) from structured (STIX, XML, JSON, CyBOX, etc.) and unstructured formats (emails, documents, web scrappers, RSS feeds, Twitter feeds, blogs, etc.).

Intel Dissemination & Actioning

- Share actionable intel with internal security teams such as IR, SOC, VAPT, Threat Hunting, and external partners within your trusted sharing network for quick actioning and analysis.
- Automate response workflows in your internal security stack such as blocking malicious IPs in Firewalls, updating SIEM data, etc.

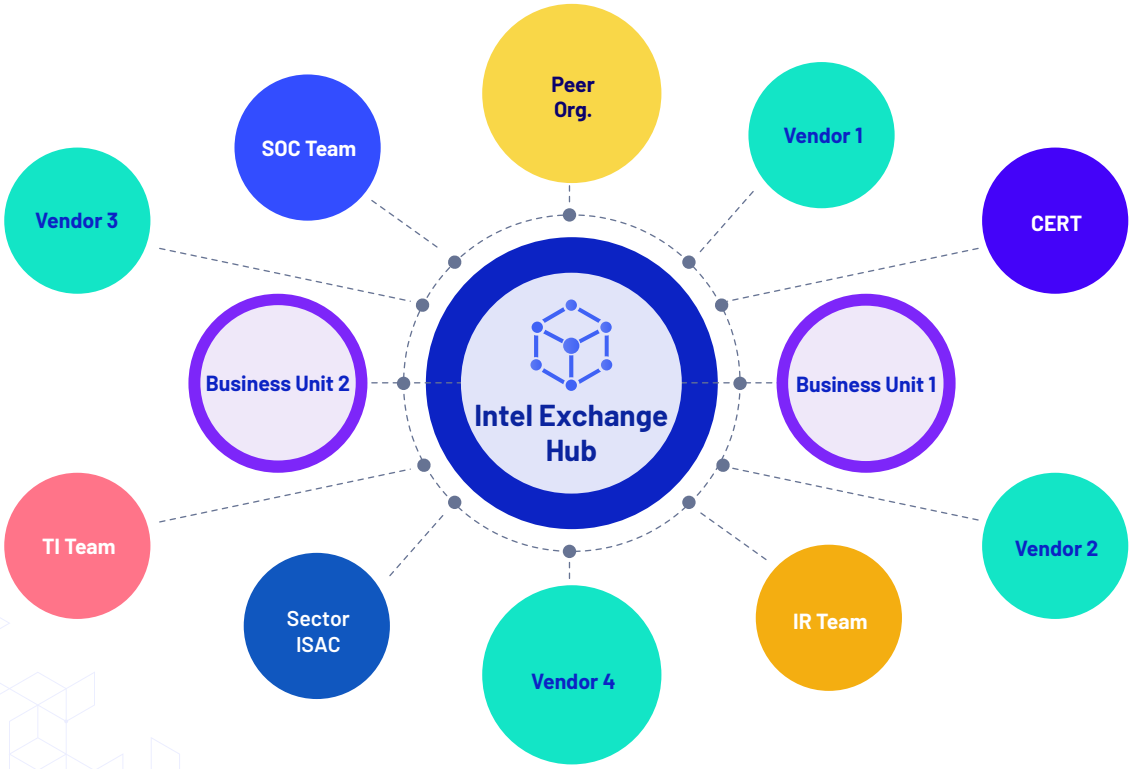
Correlation, Enrichment, and Analysis

- Automate enrichment, correlation, and analysis while performing IOC validation using the confidence scoring engine.
- Automate mundane actions using the Advanced Rules Engine & improve analysts' maturity and interoperability with automated conversion of STIX1.x (XML) to STIX 2.0 (JSON).

Governance, Collaboration, and Reporting

- Create custom reports and threat views for SOC/IR/TI teams and governance stakeholders including CISOs, Head of SOC/TI/IR, etc.
- View customized confidence scores, factor-based prioritization of cyber threats, and detailed statistical metrics within a comprehensive threat dashboard.

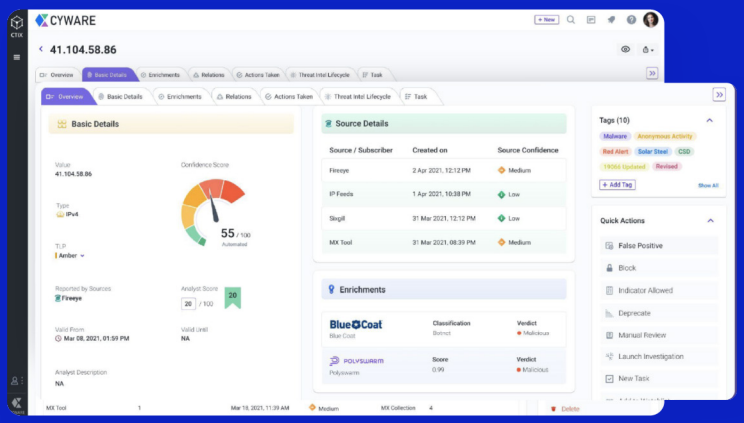
BUILD YOUR OWN TRUSTED THREAT INTEL SHARING COMMUNITY

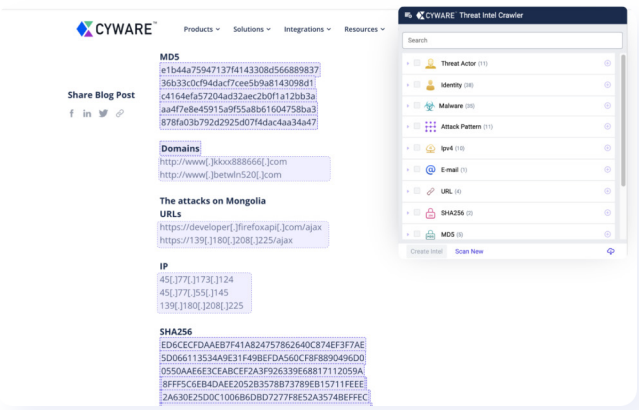


HUB-AND-SPOKE THREAT INTELLIGENCE SHARING MODEL

ADVANCED THREAT INVESTIGATIONS

- Visualize threat data like never before with a detailed view of threats, enrichments, object details, relations, and actions taken using a dedicated threat data module.
- Fetch relevant threat intelligence by writing simple queries using the in-built Cyware Query Language (CQL) search feature.
- Efficiently aggregate, analyze, and investigate massive amounts of threat data using the Diamond Model of Intrusion Analysis.





OUT-OF-THE-BOX THREAT INTEL CRAWLER

- Gather threat intelligence automatically from web pages using Intel Exchange's advanced ML and NLP capabilities.
- Save analysts' time by automatically identifying indicators, threat actors, vulnerability, malware, and attack patterns.
- Create a more enriched and contextual threat feed on the go.

THE COMPLETE ANALYST TOOLBENCH

- CENTRALIZED THREAT DASHBOARD
- DIAMOND MODEL OF INTRUSION ANALYSIS
- CYWARE QUERY LANGUAGE (CQL)
- MITRE ATT&CK NAVIGATOR
- IOC AND TTP MAPPING
- IP AND DOMAIN LOOKUP
- THREAT DATA BOARD
- STIX 1.X TO 2.X CONVERSION
- GEO-TAGGING
- MULTI-LEVEL INTEL VIEW
- ANALYST WATCHLIST
- CUSTOM REPORTING
- FINISHED INTEL REPORTS
- THREAT BULLETINS
- FANG - DEFANG
- THREAT INTEL CRAWLER (BROWSER EXTENSION)

DOCKER-BASED DEPLOYMENTS

We provide Docker-based multiple deployment options for our products, giving our customers the flexibility to make use of all the product features by choosing the best model that suits their business needs.

- PUBLIC & PRIVATE CLOUD
- ON-PREMISE
- AIR GAPPED

ABOUT CYWARE

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation SOAR (security orchestration, automation, and response) solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout.

Cyware's Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAO/CERTs and others) of all sizes and needs.

111 Town Square Place Suite 1203, #4 Jersey City, NJ 07310
cyware.com | sales@cyware.com | 855-MY-CYWARE