CYWARE™

Intel Exchange

Transform Threat Intelligence into Intelligent Action

Intel Exchange is a fully automated **Threat Intelligence Platform (TIP)** that automates ingestion, enrichment, and prioritization of threat intelligence through advanced Artificial Intelligence (AI) to transform raw data into intelligent action. Native integration with collaboration and orchestration tools enable organizations to automate actions, remediate incidents, and share, manage, and action threats proactively across siloes or trusted ecosystems.

Fig: Analyst Dashboard in Intel Exchange

End-to-End Threat Intelligence Management System

- Ingest Data from Anywhere, in Any Format
- De-duplicate and normalize data to reduce noise
- Enrich data with context and correlate
- Prioritize Threat data for Proactive Actioning
- Orchestrate Anything - Teams, silos, and security tools
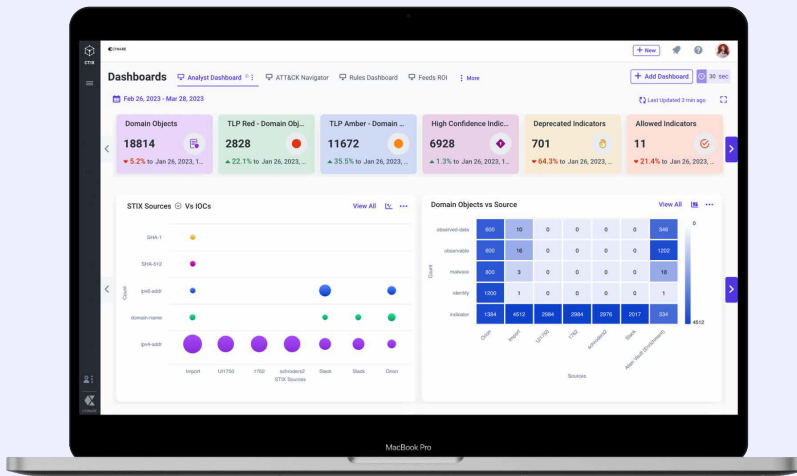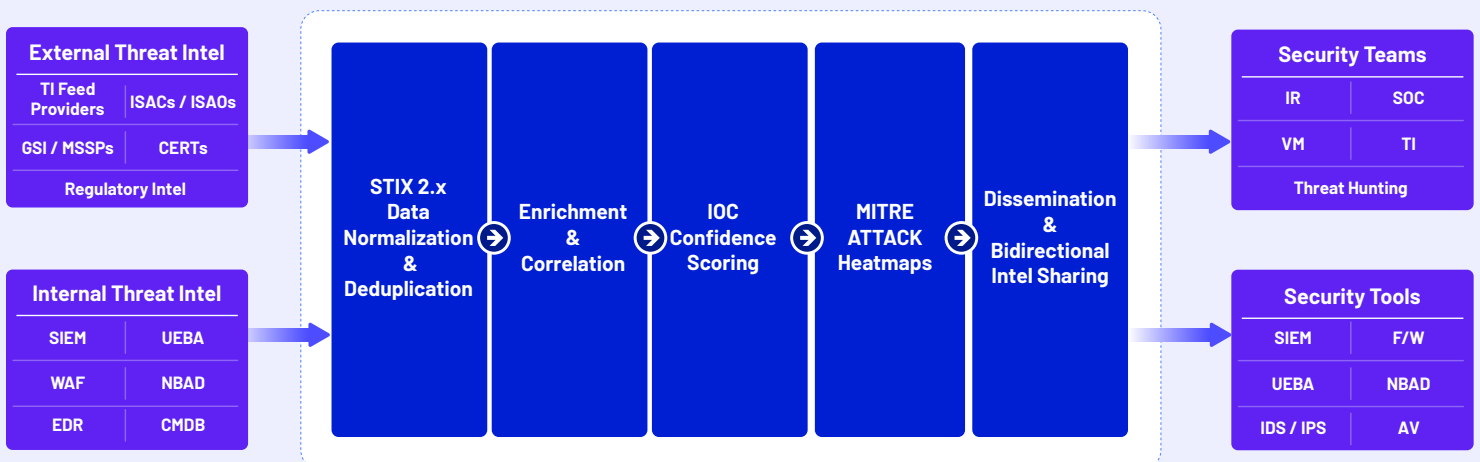- Drive collaboration and information sharing

External Threat Intel

TI Feed Providers	ISACs / ISAOs
GSI / MSSPs	CERTs
Regulatory Intel	

Internal Threat Intel

SIEM	UEBA
WAF	NBAD
EDR	CMDB

STIX 2.x Data Normalization & Deduplication → **Enrichment & Correlation** → **IOC Confidence Scoring** → **MITRE ATTACK Heatmaps** → **Dissemination & Bidirectional Intel Sharing**

Security Teams

IR	SOC
VM	TI
Threat Hunting	

Security Tools

SIEM	F/W
UEBA	NBAD
IDS / IPS	AV

Key Capabilities

INGEST

Capture all relevant threat data automatically for assured visibility

- Automated data collection of relevant threat intelligence and machine-readable IOCs from multiple source including, curated feeds, OSINT feeds, specialized premium feeds, and ISAC/CERT advisories
- Contextualized information enriched with threat actors, campaigns, and tactics, techniques, and procedures (TTPs)

MANAGE

Ingest multi-source threat intelligence into normalized, actionable data

- Deduplicate and reduce false positives to derive high-fidelity threat intelligence
- Confidence scoring for defining prioritization
- Feeds ROI calculator to optimize threat intel investments and gain visibility

INVESTIGATE

Accelerate and expedite threat visibility through threat intelligence refinement

- MITRE ATT&CK heat mapping for an actionable view of threats
- Visual threat data analysis to enrich and expand investigation
- Integrated sandbox detonation of suspicious files for investigation

ORCHESTRATE

Automate threat intelligence to action security controls

- Embedded 375+ native integrations with leading enterprise SIEMs, firewalls, EDRs, XDRs, and SOARs
- Automated inbound data ingestion and agnostic response orchestration
- Orchestration beyond incident response to inform siloed security operations

COLLABORATE

**Share and collaborate across teams, suppliers, and trusted ecosystems**

- Collaborative threat visibility sharing and awareness capability. Trusted by over 90% of ISACs
- STIX 2.x compliant for bi-directional intelligence exchange
- Comprehensive and insightful reporting and distribution to relevant stakeholders

SCALABLE

A TIP solution for any and every size security team

- Intel Exchange for large enterprise with mature threat intel programs
- Intel Exchange Lite for new or emerging threat intel programs
- Intel Exchange Spoke for small businesses desiring a managed service

---

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-PREMISES

AIR GAPPED
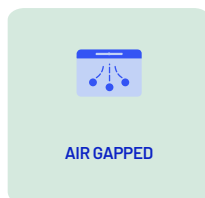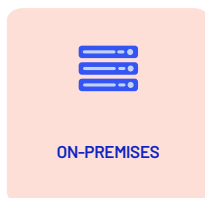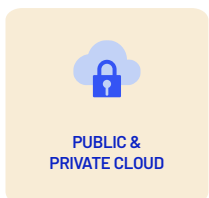
ABOUT CYWARE

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.