

Cyware Threat Intelligence eXchange (CTIX)

An Any-to-Any Threat Intelligence Analysis and Sharing Platform

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

Organizations are lacking preventive, predictive and relevant threat intelligence, which holds the key to identify, prioritize and contain threats targeting their networks and endpoints. The huge amount of threat data coming from disparate internal security tools often ends up flooding the analysis, correlation and mitigation procedures rendering them dysfunctional. To overcome these challenges, many organizations are now moving towards automated Threat Intelligence Platforms (TIPs) that act as an integrated dashboard for the ingestion, analysis, and actioning of threat data received from multiple external sources and internal security tools.

Cyware Threat Intelligence eXchange (CTIX) is an intelligent client-server exchange that leverages advanced technologies like Artificial Intelligence and Machine Learning to automatically ingest, analyze, correlate and take action upon the threat data ingested from multiple external sources and internally deployed security tools. CTIX comes with the capability to systematically convert, store and organize actionable threat data from various structured formats including STIX 1.x, STIX 2.0, XML, JSON, Cybox, OpenIOC, MAEC and unstructured formats such as Email, RSS Feeds, Threat Blogs, etc., making it a truly format-agnostic Threat Intelligence Platform.

CTIX's unique capability to ingest and action upon threat data collected from internally deployed security tools is complemented by its "Hub and Spoke" design architecture that allows organizations to create trusted sharing communities with clients, vendors, peers, affiliates, subsidiaries, ISACs/ISAOs and regulatory bodies for exchange of specific, relevant and validated cyber threat intelligence.

Capabilities and Benefits

All Source Threat Intel Ingestion

- Internal & External Intel Ingestion
- Format Agnostic IOC Conversion & Sharing
- Structured and Unstructured Intel Ingestion
- Full Subscriber and Collection Management

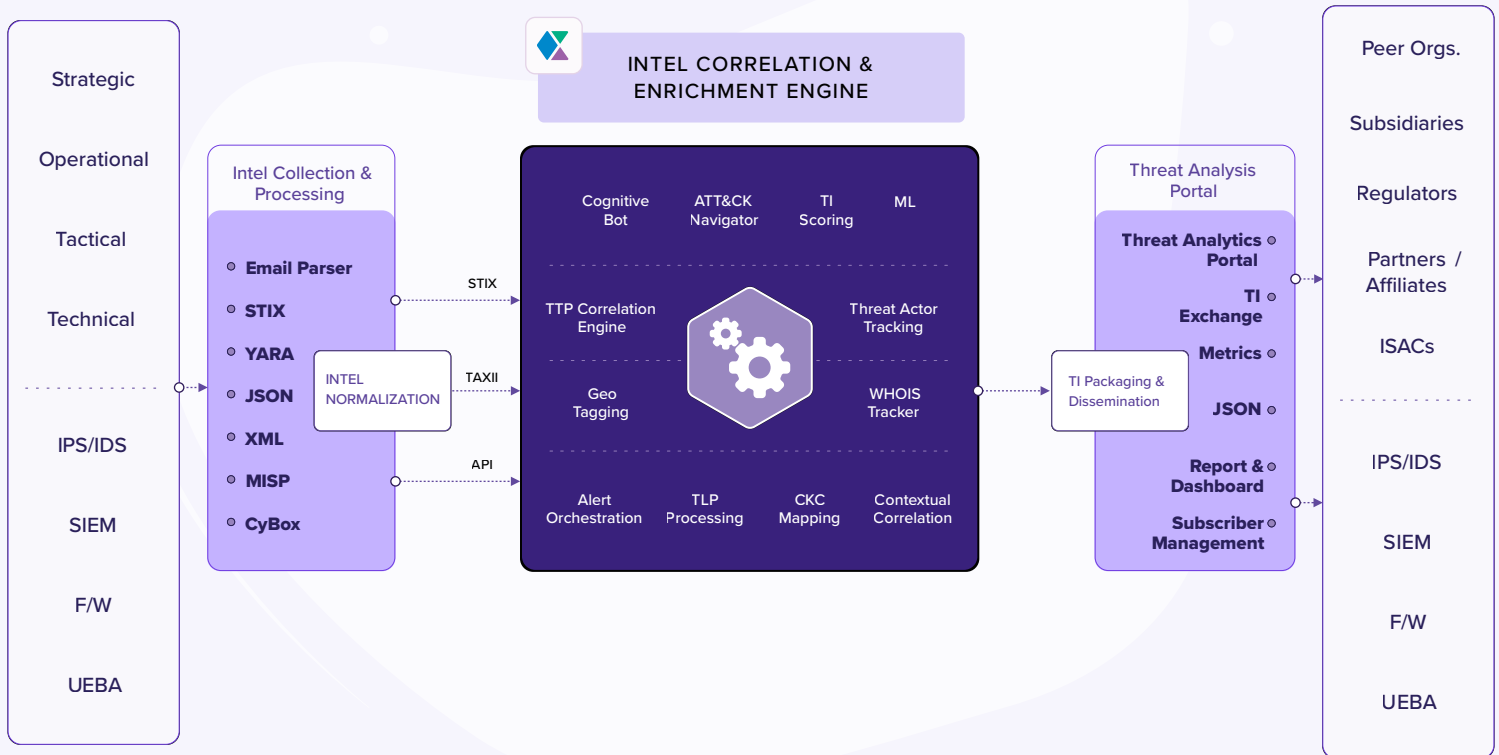
Correlation, Enrichment and Analysis

- IOC Confidence Scoring
- Advanced Rule Engine
- Machine Learning-based Analysis
- Indicator Deprecation & Threat Board

Threat Intel Dissemination and Actioning

- Internal & External Intel Dissemination
- Intel Validation & Scoring
- Intel Actioning in Firewalls, IDS/IPS, SIEMs, etc.

All processes and workflows are automated



Threat Intel Lifecycle Management

All Source Intel Collection

- Ingest Threat Intel by orchestrating with the internal security stack and trusted external sharing partners including Peers, Vendors, Subsidiaries, TI providers, CERTs, ISACs/ISAOs, Affiliates, etc.
- Automatically extract, normalize and ingest Threat Intel including IOCs in a plethora of structured and unstructured formats
- Leverage Watchlist feature to monitor relevant threats by automatically setting triggers for your organization or industry-related keywords in Threat Intel feeds

Governance & Collaboration

- Create a specialized Threat Intel view for different roles within your organization including Analysts, SOC/IR Teams, Steering Committees, and CISO
- View customized confidence scores, factor-based prioritization of cyber threats and detailed statistical metrics within a comprehensive threat dashboard
- Collaborate with your Peers, Affiliates, Subsidiaries, Vendors, etc. for automated policy-based Intel validation and scoring

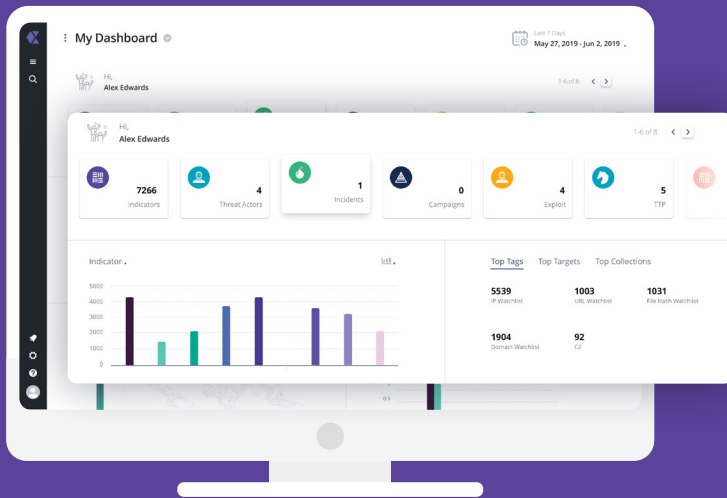
Normalization, Correlation and Enrichment

- Employ AI/ML for enrichment, correlation and deduplication of Intel feeds while removing irrelevant indicators through graduated deprecation
- Automate mundane actions to increase focus on more relevant tasks using the Advanced Rule Engine
- Improve analysts' maturity and interoperability with smooth and automated conversion of STIX1.x (XML) to STIX 2.0 (JSON)

Intel Dissemination and 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
- Use customized rules to automate response workflows in your internal security stack such as blocking of malicious IPs in Firewalls
- Track threats targeting your internal assets and receive real-time notifications and alerts vis Emails, SMS, and Calls

Build your own Trusted Intel Sharing Community

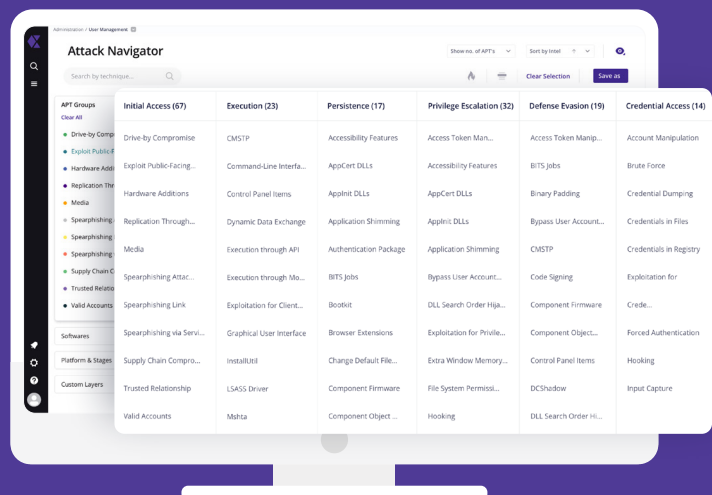


CENTRALIZED THREAT DASHBOARD

- Graphical, searchable, sortable and customizable dashboard
- Capability to quantitatively analyze all 13 STIX Objects
- Easy pattern analysis and threat identification with customized graphs
- Live Stats Visualizer for faster threat detection

MITRE ATT&CK NAVIGATOR

- Identify threats lurking in your environment by mapping Indicators of Compromise (IOCs) to various APT Tactics, and Techniques
- Visualize gaps in your network defenses by gaining insights into tools and attack patterns leveraged by Advanced Persistent Threats (APTs)
- Create your own ATT&CK layers for advanced threat mapping and malicious code analysis



The Complete Analyst Workbench

ATT&CK NAVIGATOR	Visualize Tactics, Techniques and Procedures (TTPs) of Advanced Persistent Threats (APTs) using MITRE's ATT&CK Navigator
IP AND DOMAIN LOOKUP	Integrate with services like WHOIS, VirusTotal, Shodan, Moz, and GeoIP to empower your analysts in accessing data collected from premium sources with a single click
THREAT BOARD	Search object types, indicator types and hidden cross-links between different attributes extracted from disparate Threat Intel feeds
STIX 1.X TO STIX 2.0 CONVERSION	Ensure advanced threat data interoperability with smooth conversion of STIX 1.x (XML) to STIX 2.0 (JSON)
GEO-TAGGING	Map and analyze Threat Intel automatically ingested from disparate sources to identify geographical trends for your different business units
MULTI-LEVEL INTEL VIEW	Create a specialized Intelligence view for different roles within your organization including Analysts, SOC/IR Teams, Steering Committees, and CISO
ANALYST WATCHLIST	Monitor relevant threats by setting triggers for your organization or industry-related keywords in intelligence feeds
CENTRALIZED THREAT DASHBOARD	View customized confidence scores, factor-based prioritization of cyber threats and detailed statistical metrics within a comprehensive platform
FANG-DEFANG	Obfuscate malicious indicators to make them ineffective if inadvertently clicked or automatically processed in error

Deployment Environments

We provide 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 and Private Cloud



On-Premise



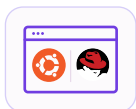
Hybrid



Air Gapped

System Requirements

System requirements will change based on the considerations of high availability and backups.



Operating System



CPU Cores



Memory



Storage

About Cyware

Cyware Labs is a product-based cybersecurity provider headquartered in New York, USA. Cyware offers a full-stack of innovative cyber fusion solutions for strategic, tactical, technical and operational threat intelligence sharing, security automation and full threat response.


Cyware's solutions are designed to inculcate cyber resilience and promote secure collaboration between organizations. Cyware's products while enhancing threat visibility, also deliver the needed control for a proactive response by providing organizations with an automated context-rich analysis of threats without losing the element of human judgment.



Cyware®

1460 Broadway New York NY 10036

cyware.com | sales@cyware.com

 855-MY-CYWARE

