The inability to ingest, analyze and make threat intelligence actionable 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 respond to threats targeting their networks and endpoints. The high volume 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, organizations require an automated threat intelligence platform (TIP) that acts 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 such as artificial intelligence and machine learning to automatically ingest, analyze, correlate, and act upon the threat data collected 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, and others, making it a truly format-agnostic TIP.

CTIX’s unique capability to ingest and act upon threat data collected from internally deployed security tools is complemented by its “hub and spoke” architecture. This framework allows organizations to create trusted sharing communities with clients, vendors, peers, affiliates, subsidiaries, ISACs/ISAOs, and regulatory bodies exchanging specific, relevant, and validated cyber threat intelligence.

**Capabilities and Benefits**

### All-Source Threat Intel Ingestion
- Internal and External Threat Intel Ingestion
- Format Agnostic Indicator Conversion and Sharing
- Structured and Unstructured Intel Ingestion
- Full Subscriber and Collection Management

### Correlation, Enrichment, and Analysis
- Customizable IOC Confidence Scoring
- Advanced Intel Automation Rule Engine
- Machine Learning-based Analysis
- Indicator Deprecation and Threat Board

### Threat Intel Dissemination and Actioning
- Internal and External Intel Dissemination
- Automated Intel Validation and Scoring
- Intel Actioning in Firewalls, IDS/IPS, SIEMs, etc.
- Rule-Based Advanced Alerting and Notifications
All Source Intel Collection

- Ingest threat intelligence 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 variety 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.

Normalization, Correlation, and Enrichment

- Automate the enrichment, correlation, and deduplication of intel feeds while removing irrelevant indicators through graduated depletion.

- 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).

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, and other stakeholders for automated policy-based intel validation and scoring.

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 via emails, SMS, and voice alerts.
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 IOCs to various APT TTPs
- Visualize gaps in your network defenses by gaining insights into the tools and attack patterns leveraged by APTs
- Create your own ATT&CK layers for advanced threat mapping and malicious code analysis
### The Complete Analyst Workbench

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATT&amp;CK NAVIGATOR</td>
<td>Visualize tactics, techniques, and procedures (TTPs) of APTs using MITRE's ATT&amp;CK Navigator.</td>
</tr>
<tr>
<td>IP AND DOMAIN LOOKUP</td>
<td>Integrate with services such as WHOIS, VirusTotal, Shodan, Moz, and GeoIP to empower your analysts to enrich data with a single click.</td>
</tr>
<tr>
<td>THREAT BOARD</td>
<td>Search object types, indicator types, and hidden cross-links between different attributes extracted from disparate threat intel feeds.</td>
</tr>
<tr>
<td>STIX 1.X TO STIX 2.0 CONVERSION</td>
<td>Ensure advanced threat data interoperability with smooth conversion of STIX 1.x (XML) to STIX 2.0 (JSON).</td>
</tr>
<tr>
<td>GEO-TAGGING</td>
<td>Map and analyze threat intel automatically ingested from disparate sources to identify geographical trends for your different business units.</td>
</tr>
<tr>
<td>MULTI-LEVEL INTEL VIEW</td>
<td>Create a specialized intelligence view for different roles within your organization including analysts, SOC/IR teams, steering committees, and CISO.</td>
</tr>
<tr>
<td>ANALYST WATCHLIST</td>
<td>Monitor relevant threats by setting triggers for your organization or industry-related keywords in intelligence feeds.</td>
</tr>
<tr>
<td>CENTRALIZED THREAT DASHBOARD</td>
<td>View customized confidence scores, factor-based prioritization of cyber threats, and detailed statistical metrics within a comprehensive platform.</td>
</tr>
<tr>
<td>FANG-DEFANG</td>
<td>Obfuscate malicious indicators to make them ineffective if inadvertently clicked or automatically processed in error.</td>
</tr>
</tbody>
</table>

### Deployment Environments

We provide multiple deployment options for our products, giving our customers the flexibility to utilize all our product features by choosing the model that best 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 provides threat intelligence sharing and cyber fusion products to security teams across the world. Cyware’s innovative solutions include capabilities for strategic and tactical threat intelligence sharing, cyber fusion, security orchestration, and incident response. Cyware’s solutions make secure collaboration, cyber resiliency, and enhanced threat visibility a reality for customers.