CTIX Lite™

Introducing the First Fully Automated, Lightweight Threat Intel Platform (TIP) for Small to Mid-sized Security Teams

CTIX Lite is a comprehensive solution with premium feeds, enrichment, and automation in a single platform. By combining premium threat intelligence feeds and enrichment sources in an easy-to-use threat intelligence automation platform, teams of all sizes and budgets can now improve the speed and accuracy of their security operations. This complete, all-in-one solution enables automation throughout the threat intelligence lifecycle to accelerate a proactive defense against threats, and all for one-fifth of the cost of other enterprise TIPs.

Threat Intel Automation Platform Pre-Loaded with Premium Intelligence Feeds and Enrichment Sources

FLASHPOINT

BAMBENEK LABS

POLYSWARM

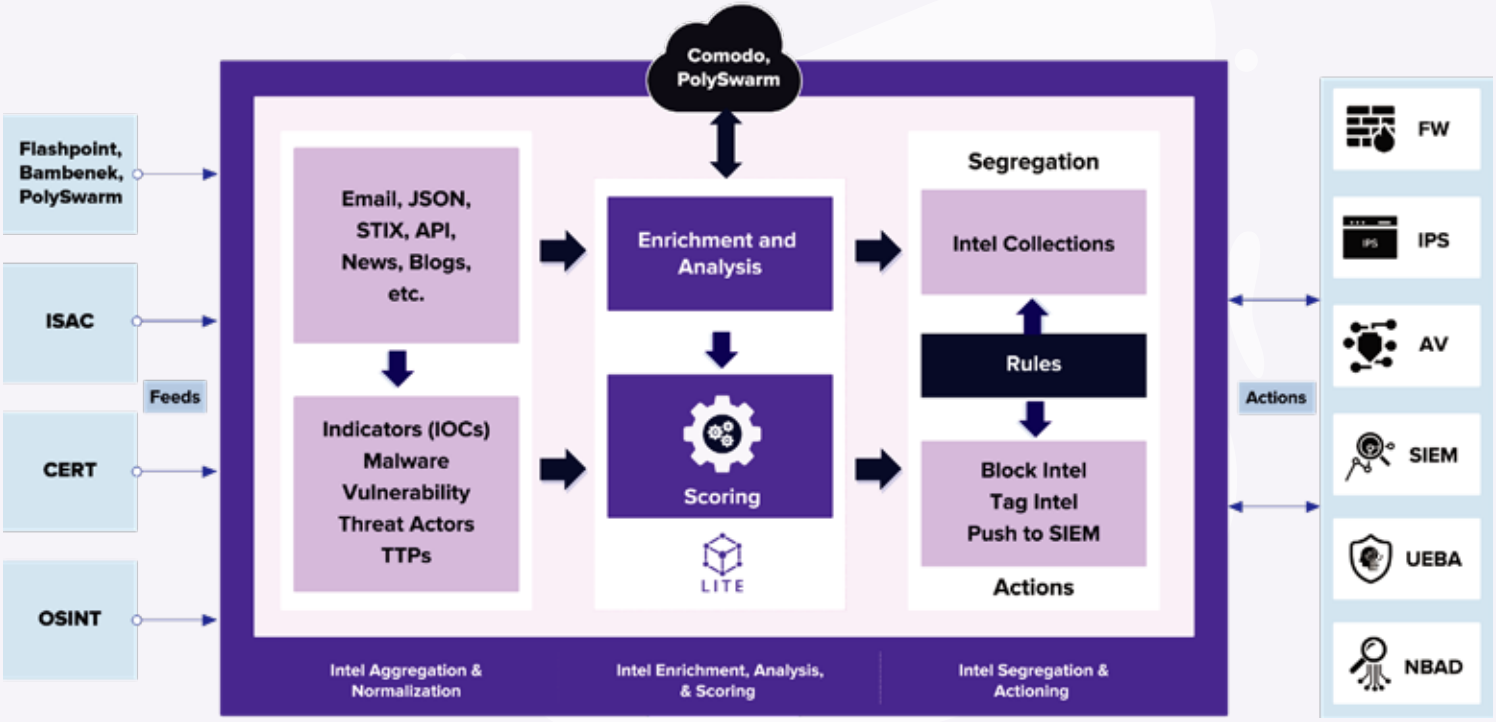
COMODO

**More intel feeds and enrichment sources to be added soon*

Finally, a Threat Intelligence Solution for Teams that:

- Do not have (or have a very small) threat intel team
- Do not have a large cybersecurity budget for costly TIPs
- Receive and share intel with one or more ISACs or ISAOs
- Ingest threat data from multiple dark web or OSINT sources
- Receive threat intel in emails or files and process it manually
- Need the capability to operationalize threat intelligence faster

Ingest, Analyze, and Act on Relevant, Enriched Intelligence



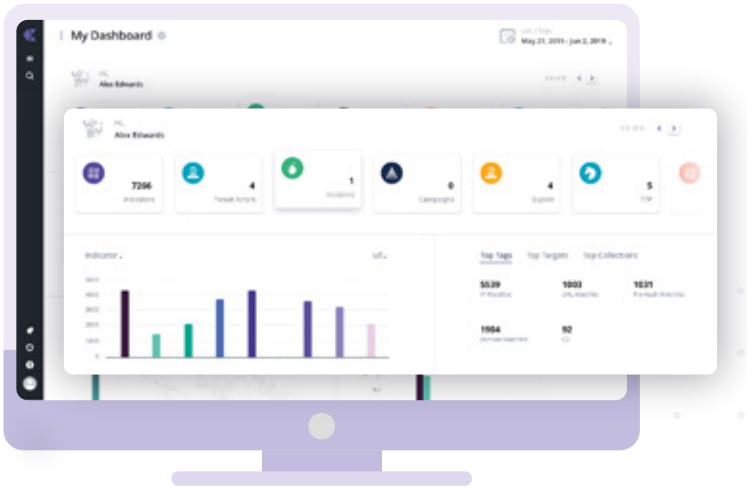
Detect Threats Faster with Advanced TIP Features

- Collect threat intelligence from multiple sources (ISACs, OSINT, Dark Web)
- Ingest threat indicators (IOCs) in STIX format
- Process unstructured threat intelligence received from emails, reports, and blogs
- Automate end-to-end threat intel workflows – ingestion through actioning
- Threat intel feeds that never expire – Flashpoint, Bambenek, Polyswarm
- Enrich your data for no additional charge – Polyswarm, Comodo
- Simple yet powerful automation with custom confidence scoring for indicators
- Update your SIEM records without writing complex playbooks
- Integrate and take actions in your security tools

Automate Threat Intel Workflows for Faster, Smarter Security

- Automate threat intelligence ingestion, enrichment, and contextualization
- Automate SIEM lookup and reference for future threat detection and monitoring
- Automate blocking of IOCs on security technology such as firewall, AV, IPS, etc.
- Assign high priority indicators and threats to analysts for manual review

Increase Efficiency Through Easy-to-Use Automation

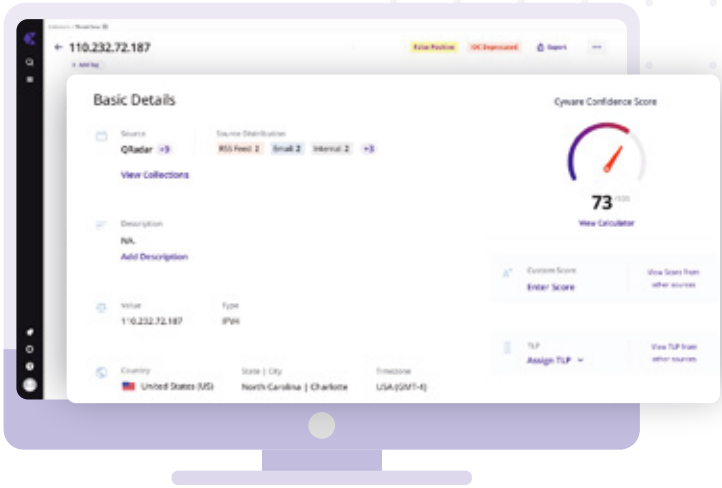


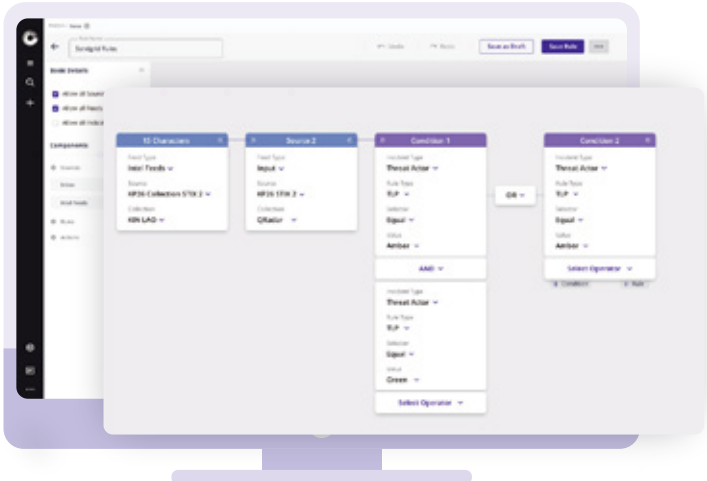
ADVANCED DASHBOARD

- Visualize threat data to gain a high-level understanding of your threat intelligence operations and underlying security threats.
- Track critical security metrics with the readily available widget library.
- Continuously monitor the flow of threat intelligence across your security operations workflows.

SIMPLIFY SECURITY OPERATIONS

- Automatically ingest and parse structured and unstructured intelligence
- Enrich data with additional context from Polyswarm and Comodo
- Take actions on internal cloud or on-premise hosted SIEM using pre-defined automation rules





AUTOMATION RULES

- Automate threat intelligence lifecycle workflows and processes including ingestion, normalization, enrichment, analysis, and dissemination.
- Trigger automated actions directly in your deployed security technologies such as SIEM, firewalls, etc.
- Automate mundane workflows, speed up triage management and enable security teams to focus more on relevant tasks.

Premium Feeds & Enrichment Sources

Premium Feeds

Flashpoint IOCs and CVEs - Premium intelligence from Flashpoint with indicators of compromise (IOCs) and technical data across Flashpoint datasets.

PolySwarm - A real-time stream of new and emergent malware with a focus on new Ransomware Families of which over 25% of the files are not yet in competing feeds.

Bambenek IP and Domain Feed - A Self-curating feed that monitors malicious networks to observe the current criminal activity.

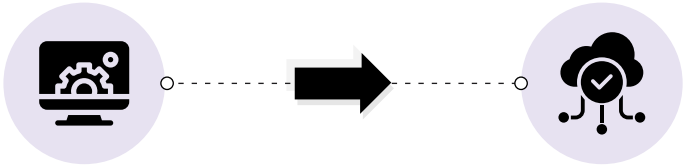
Cyware Threat Feed - Threat data collected from a wide variety of open and trusted sources to deliver a consolidated stream of actionable threat intelligence.

Enrichment Sources

Comodo Enrichment - Comodo Valkyrie is a cloud-based, verdict-driven platform that provides static, dynamic and as needed, expert human analysis for submitted unknown and zero-day files. The Valkyrie verdict system analyzes over 200 million file queries per day and more than 300 million unknown files each year through tightly integrated Comodo solutions and our active global community of threat researchers.

PolySwarm Enrichment - PolySwarm is a launchpad for new technologies and innovative threat detection methods, that provides file enrichment supplied by a crowd-sourced network of research-driven, anti-malware solutions, with superior accuracy against the latest malware.

30-Minute Cloud Deployment



- Easy to deploy and set up, reducing onboarding lead time.
- Effective cost saving along with the ability to easily scale the application.
- Increased redundancy and efficient disaster recovery environment.

About Cyware

Cyware offers the technology organizations need to build a virtual cyber fusion center. With separate but integrated solutions including an advanced threat intel platform (TIP), vendor-agnostic security automation (SOAR), and security case management, organizations are able to increase speed and accuracy while reducing costs and analyst burn out. Cyware's solutions make secure collaboration, cyber resiliency, and enhanced threat visibility a reality for customers.

CYWARE™

Cyware®

228 Park Ave S, #77147, New York, New York 10003-1502

cyware.com | sales@cyware.com

855-MY-CYWARE