CYWARE™

Intel Exchange Lite

Intel Exchange Lite

A Cloud-Native, Automated Threat Intelligence Platform (TIP) for Growing Teams

Intel Exchange Lite is a comprehensive TIP solution for mid-market security teams that comes loaded with industry-popular threat intel feeds, enrichment, and automation in a single platform. By combining industry-popular threat intel feeds and enrichment sources in an easy-to-use threat intelligence automation platform, growing security teams can now collaborate better and improve the speed and accuracy of their security operations. This complete, all-in-one solution enables automation throughout the threat intelligence lifecycle to accelerate proactive defense against threats, and all for a fraction of the cost of other enterprise TIPs.

ENABLE FASTER, LAST-MILE THREAT INTEL OPERATIONALIZATION

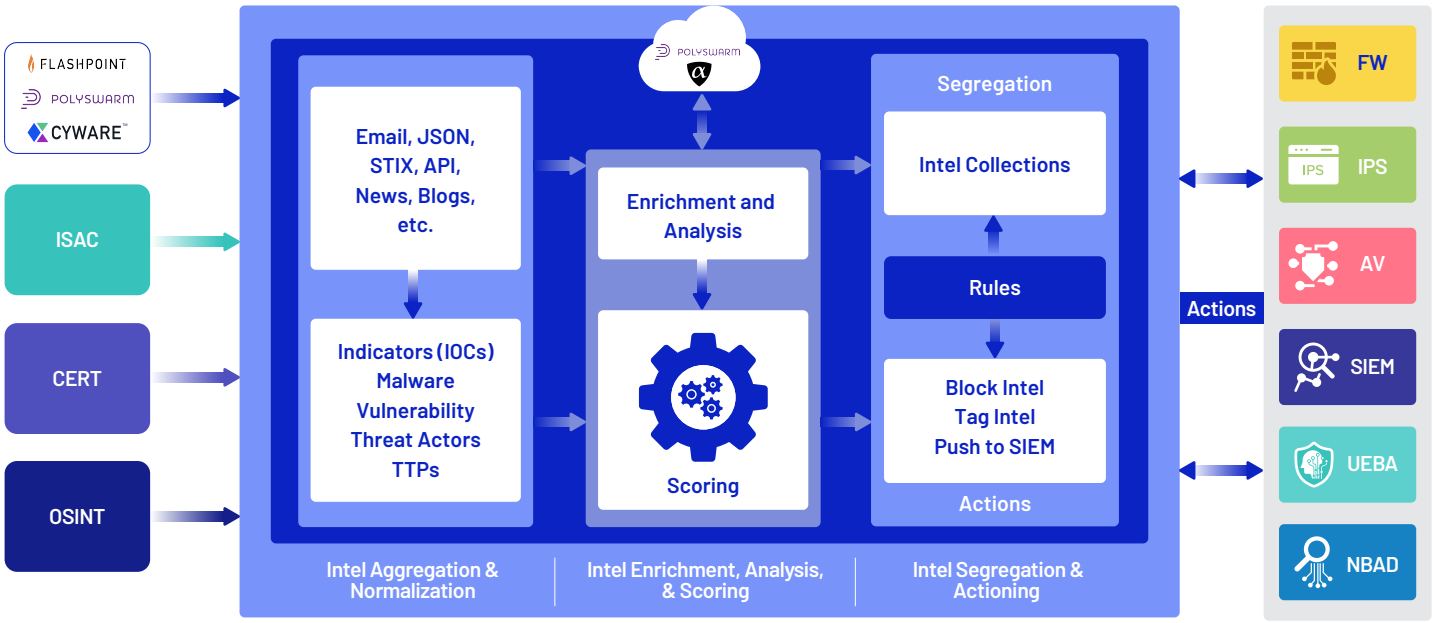
- Multi-source threat intel ingestion
- Bi-directional sharing with ISACs/ISAOs
- Automation rules for STIX-based sharing
- Pre-built SIEM connectors for end-to-end sharing and actioning
- Pre-loaded threat intel feeds and enrichment sources
- Pre-loaded high fidelity Cyware threat intel feed

LOOK NOWHERE ELSE: Intel Exchange Lite comes with Pre-Loaded Threat Intelligence and Enrichment

FLASHPOINT	POLYSWARM	alphaMountain	CYWARE™
Threat Intel Feed	Threat Intel Feed Enrichment	Enrichment	Threat Intel Feed

Intel Exchange Lite is designed for mid-sized security teams that are unable to use advanced threat intelligence platforms (TIPs) due to budget or team constraints. If you are a large enterprise, please reach out to our sales team for our advanced TIP offering at sales@cyware.com.

INGEST, ANALYZE, AND ACT ON RELEVANT, ENRICHED INTELLIGENCE



DETECT AND ANALYZE 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 (Emails, Reports, and Blogs)
- Take automated actions on threat data using custom confidence scoring
- Integrate and take actions in your security tools
- Perform advanced threat investigation and search using Cyware Query Language (CQL)
- Create personalized and enriched custom reports for centralized governance and visibility
- Update your SIEM records without writing complex playbooks

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

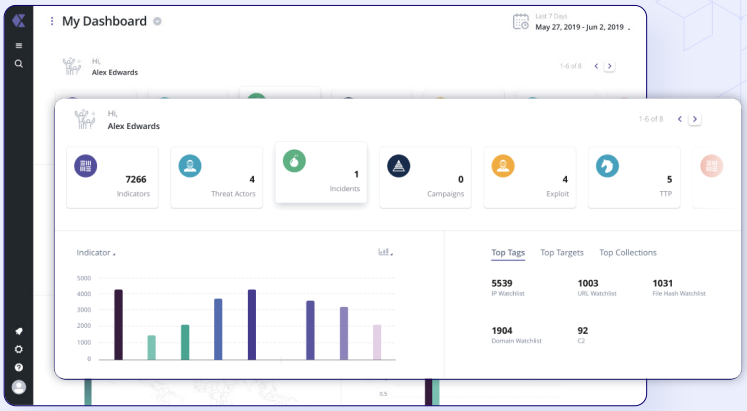
Automate blocking of IOCs on security technology such as firewall, AV, IPS, etc.

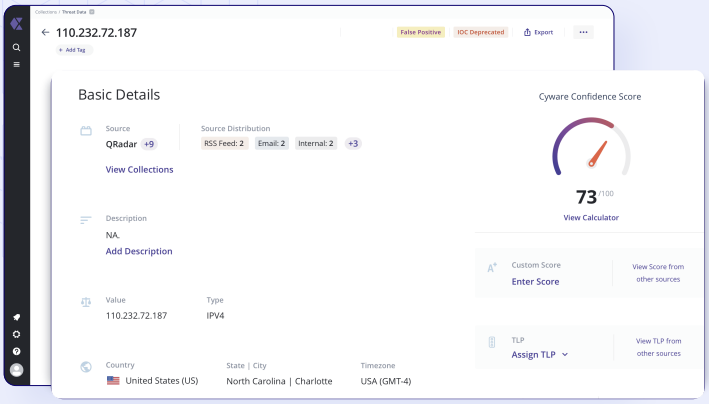
Assign high priority indicators and threats to analysts for manual review

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 operation workflows.



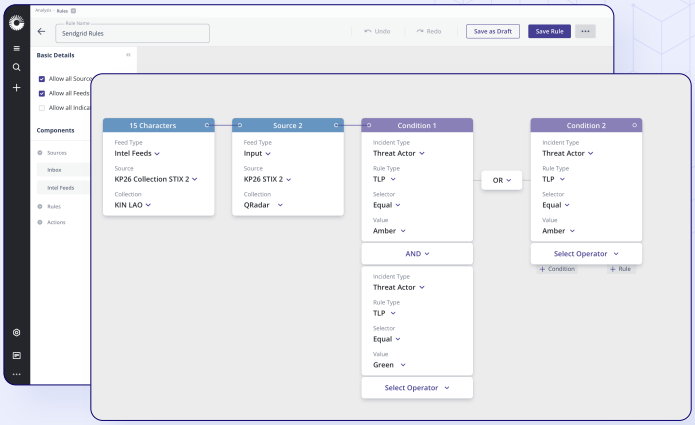


Simplified Security Operations

- Automatically ingest and parse structured and unstructured threat intel from multiple sources including pre-loaded threat intel feeds from Flashpoint, PolySwarm, and Cyware.
- Deduce contextual intel through inbuilt confidence scoring engine and external enrichment via PolySwarm and alphaMountain.
- Create and schedule customized reports for SOC/IR/TI teams and governance stakeholders including CISOs, Head of SOC/TI/IR, etc.

Automation Rules Engine

- 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, EDR, firewalls, etc.
- Automate mundane workflows, speed up triage management and enable security teams to focus more on relevant tasks.



THREAT FEEDS AND ENRICHMENT SOURCES

THREAT 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.

Cyware Threat Feed

A self-curating feed that monitors malicious networks to observe ongoing cyber criminal activity and delivers a consolidated stream of actionable threat intelligence.

ENRICHMENT SOURCES

alphaMountain

The alphaMountain threat intelligence integration enables users to conduct investigations informed by the risk scores and relevant content categorization of hosts, domains, IP addresses, and URLs. Organizations can enrich domains/URLs with a daily limit of 25k API calls.

PolySwarm Enrichment

PolySwarm is a launchpad for new technologies and innovative threat detection methods, that provides file enrichment supplied by a crowdsourced network of research-driven, anti-malware solutions, with superior accuracy against the latest malware. Organizations can enrich upto 20k hashes/month and upto 700 hashes/day.

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 resilience and efficient disaster recovery environment.

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