Cyware Intel Packaged Solution

Industry-First Threat Intel Packaged Solution, now with Compromised Credential Management
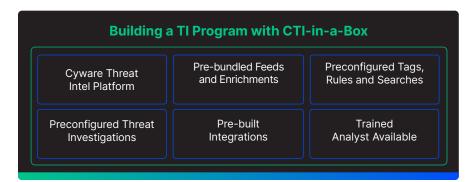
The Challenge

Security teams today are overwhelmed by the complexity and time it takes to launch or scale cyber threat intelligence (CTI) programs. Sourcing multiple vendor solutions, integrating disparate intel feeds, configuring enrichment rules, building response workflows, and aligning internal stakeholders often takes months - delaying threat visibility and leaving organizations vulnerable.

Early-stage CTI programs often lack the internal resources, integrations, and automation to get off the ground efficiently. Moreover, security teams often struggle to detect critical exposure risks like compromised credentials, infostealer malware, and phishing campaigns targeting their brand or employees. The result? A fragmented, manual, and slow-moving threat detection and response capability that puts organizations at risk and analysts under constant pressure.

The Solution

The Cyware Intel Packaged Solution is a fully pre-configured threat intel program that lets security teams bypass months of setup and start detecting and responding to threats within days. Built on the proven Cyware Intel Exchange platform, the solution adds new exposure management capabilities with Compromised Credential Management (CCM), pre-integrated Team Cymru threat feeds, Cyware Quarterback AI-powered chat assistant, pre-configured tags, dashboards, and more.

It empowers security teams to skip the heavy lifting and start operationalizing threat intelligence from day one by eliminating the operational hurdles of integration, enrichment, and response configurations so your analysts can focus on action, not setup.

Building a TI Program with CTI-in-a-Box

Cyware Threat Intel Platform	Pre-bundled Feeds and Enrichments	Preconfigured Tags, Rules and Searches
Preconfigured Threat Investigations	Pre-built Integrations	Trained Analyst Available

Key Benefits

Accelerated Time-to-Value: Launch your CTI program in days, not months, bypassing the resource-intensive steps of configuring threat feeds, enrichment sources, workflows, and dashboards.

Single Hub for All Threat Intel Requirements: Unify your threat intel operations through a centralized platform that incorporates diverse intel sources and covers end-to-end use cases, from ingestion and enrichment to advanced correlation, analysis, threat sharing, exposure management, and automated response.

Streamlined CTI Program Maintenance: Reduce operational complexity with built-in enrichment connectors, pre-configured dashboards, intel tags, saved searches, and automation rules curated by Cyware's CTI experts.

What's Inside the Solution

Cyware Intel Exchange — Unified Threat Intelligence Platform
At the core of the solution is Cyware Intel Exchange—a fully automated Threat Intelligence Platform (TIP) that manages the full threat intel lifecycle.

- Format-agnostic ingestion from OSINT, commercial feeds, ISACs, and internal sources
- Deduplication, normalization, and correlation with contextual enrichment
- Confidence scoring, auto-tagging, and MITRE ATT&CK mapping
- Rule-based automation and cross-tool intel distribution
- Real-time STIX 2.x sharing with partners, suppliers, and internal teams

Exposure Management — Compromised Credential Management (CCM)
Included in the package, the exposure management module adds continuous credential exposure monitoring and remediation abilities.

- Scan the surface, deep, and dark web for leaked credentials tied to your domains
- Detect infostealer malware activity and impersonation attempts
- Integrate with IAM tools for breach risk categorization
- Automate remediation via playbooks or trigger immediate manual actions

Cyware Quarterback — AI-powered Cybersecurity Chat Assistant
Transform threat intelligence operations by automating detection and response workflows to execute complex tasks with speed and precision.

- Ask questions in plain language and get structured, actionable answers
- Integrate with top security tools, platforms, and knowledge bases
- Cut investigation time by 50%+ with AI-driven enrichment
- Access cited insights from Cyware docs and trusted OSINT sources

Pre-Configured CTI Workflows, Tags, and Dashboards
Jumpstart your threat intel program with ready-to-use operational content curated by Cyware's CTI experts.

- Tagging logic, saved searches, and dashboards aligned to common use cases
- Role-based views for analysts, SOC managers, and executives
- No requirement of custom scripting to go live

Team Cymru Premium Threat Feeds
Pre-integrated with Intel Exchange, these feeds provide deep visibility into global adversary infrastructure and malware campaigns.

- 50B+ flow records and 150K+ tracked C2 addresses monitored daily
- Visibility into botnets, phishing domains, and malware infrastructure
- Enrich internal indicators with geograpy, threat actor, and campaign metadata

Smart Capabilities. Strong Outcomes.

Real-Time Threat Visibility
Leverage Team Cymru threat feeds to uncover malware infrastructure, phishing domains, and botnet traffic, fueling more effective detection and triage.

Proactive Credential Risk Management
Detect and respond to compromised credentials with IAM-ready risk categorization and playbook automation.

AI-Accelerated Threat Investigations
Get structured and actionable insights in seconds, access cited insights from Cyware docs and OSINT sources, and integrate with third-party tools.

About Cyware
Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation security orchestration and automation solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Cyber Fusion solutions enable secure collaboration, information sharing, and enhanced threat visibility for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAO/CERTs and others) of all sizes and needs.