CYWARE™ | Solution Brief

Cyware Intelligence Suite

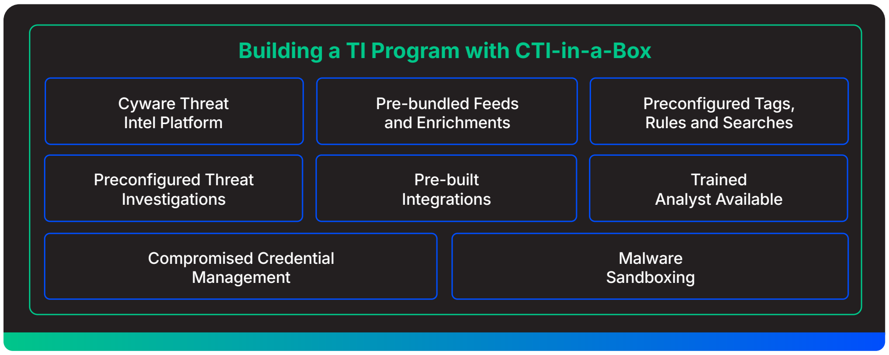
The First CTI Program-in-a-Box, Now Enhanced with Native Sandboxing, Sector-Specific Malware Intel, and Dark Web Domain Sightings

The Challenge

Launching or scaling a CTI program can take months of stitching together feeds, enrichment sources, sandboxes, and response tools, often leaving blind spots around malware behaviour, dark-web threats, and credential leaks. Without built-in automation or AI, analysts drown in low-context IOCs and manual workflows that delay response. The Cyware Intelligence Suite was created to eliminate these hurdles and deliver immediate, measurable security outcomes.

The Solution: Cyware Intelligence Suite

The Cyware Intelligence Suite 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 Cyware Intelligence Suite offers native sandboxing, curated sectoral and malware infrastructure threat feeds, integrated exposure management, and AI-driven enhancements so that teams can operationalize threat intelligence rapidly and effectively.



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
- Compromised Credential Management
- Malware Sandboxing

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.

CYWARE™

What’s Included in the Suite

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
- Custom risk scoring, auto-tagging, and MITRE ATT&CK mapping
- AI-driven quick intel parsing, threat summaries, and web intel crawler
- Rule-based automation and cross-tool intel distribution
- Real-time STIX 2.x sharing with partners, suppliers, and internal teams

Native Malware Analysis Sandbox

A built-in, multi-engine sandbox (CAPE & Triage) that detonates Windows, Linux, and Android samples and provides rich artifacts and MITRE ATT&CK-mapped TTPs back into Cyware Intel Exchange.

- Multi-engine analysis with flexible VM images and configurable internet access
- Automatic extraction of hashes, network IOCs, and ATT&CK-aligned TTPs for instant correlation
- Rich artifact downloads (PCAP, memory dump, configs, screenshots) drive rapid detection tuning and threat hunting

Cyware Sectoral Feeds

A curated, daily-updated collection of malware and ransomware IOC feeds that deliver enriched hashes with static (PEFile, ExifTool) and behavioural (CAPE, Triage) analysis across eight vertical feeds.

- Sector-aligned IOCs for Healthcare, Finance, Energy, Government, Manufacturing, and Operational Technology (OT)
- Gain static and behavioural context and AV scan results to accelerate triage and enrichment
- Indicators mapped to malware families, MITRE TTPs, and related IPs, domains, and URLs for deeper investigation

Exposure Management for Compromised Credentials and Domain Sightings

A unified Exposure Management module that combines Compromised Credential Management with Domain Sightings to monitor leaked credentials, infostealer-malware dumps, and dark-web references to corporate domains.

- Prevent account takeover with automatic password resets or token revocation via IAM.
- Detect phishing, brand abuse, and domain spoofing early through automated domain monitoring.
- Correlate exposure events with malware, TTPs, and infrastructure intel for faster investigations.

Team Cymru Threat Feeds

Near real-time telemetry on botnets, command-and-control servers, and malicious infrastructure, sourced from a global sensor network.

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

Smart Capabilities. Strong Outcomes.

See Faster, Act Sooner

Sector-aligned malware feeds, real-time malware infrastructure telemetry, and native sandboxing deliver contextual intel in hours, not weeks, so threats are identified and triaged before attackers gain traction.

Automate the Heavy Lifting

AI-driven intel parsing and summarization, along with rule-driven enrichment and actioning, helps analysts push high-confidence IOCs, compromised credentials, and domain sightings to SIEM, SOAR, EDR, and IAM without manual efforts.

Simplify & Scale

One unified platform replaces scattered point tools, cuts integration costs, and scales effortlessly from a single team to distributed environments under one contract and SLA.

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.

cyware.com

sales@cyware.com

111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310