CYWARE™ | Microsoft Solution Brief

Cyware and Microsoft
Driving Advanced Threat Intelligence for Enhanced SecOps and Collective Defense

The Threat Intelligence Operations Challenge

Cyber threats are evolving faster than ever, and every intelligence discovery matters. Insights from one organization can strengthen defenses across the broader security community for enhanced resilience.

Traditional approaches have limited this potential. While threat intelligence (TI) flowed into Security Information and Event Management (SIEM) solutions via Threat Intelligence Platforms (TIPs), environment-specific insights generated within the SIEM often remained isolated and underutilized. The industry left it as a one-way workflow.

Microsoft and Cyware Integration Solves It

As an **Azure IP Co-Sell partner,** Cyware's strategic alliance with Microsoft removes these barriers. Combining Cyware's AI-powered threat intelligence automation with Microsoft Sentinel's cloud-native SIEM capabilities enables **bi-directional threat intelligence exchange via STIX/TAXII.** This new architecture enables the critical reverse flow, allowing intelligence generated within Microsoft Sentinel to be automatically shared back with Cyware Intel Exchange.

This automated, real-time flow allows security teams to operationalize intelligence faster, and eliminate challenges like siloed data, inconsistent context, and manual handoffs. Together, these advancements enable security teams to move from fragmented defense to unified collective defense.

Cyware Intel Exchange also integrates with Microsoft Defender, enabling ingestion and enrichment of Defender threat intelligence feeds, automating indicator searches to accelerate triage and investigation, and triggering automated response actions within Defender for Endpoint.

The deep product integrations between Cyware and Microsoft enable you to:

- **Accelerate threat detection and response**
- **Share enriched threat intelligence seamlessly**
- **Gain actionable insights for faster decision-making**
- **Strengthen unified security operations and collective defense**

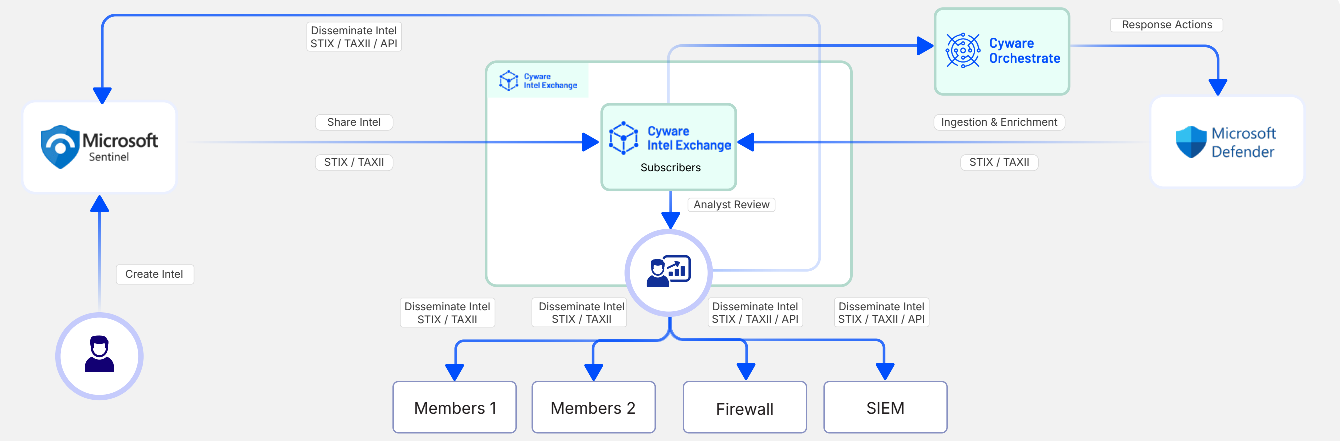

FIGURE 1. *Bi-Directional Threat Intelligence Sharing Architecture Between Microsoft and Cyware*

CYWARE™

Accelerate Unified Threat Intelligence Operationalization and Enable Stronger Collective Defense Across Your Ecosystem

As a Microsoft Azure IP Co-Sell partner, Cyware's solutions are available in the Azure Marketplace.

This collaboration provides an **integrated threat intelligence workflow** across Cyware Intel Exchange, Microsoft Sentinel, and Microsoft Defender for Endpoint, giving security teams a faster path from insight to action.

It also supports Azure-hosted deployment options for customers standardizing on Microsoft, ensuring a **scalable and unified approach** to threat detection and response.

Key Use Cases

CYWARE + Microsoft Sentinel

Bi-Directional Threat Intelligence Sharing

Automatically share real-time intelligence, including IOCs and sightings, between Sentinel and Cyware Intel Exchange, with support for STIX/TAXII-based sharing, reducing time-to-action from hours to minutes.

Collective Defense Enablement

Receive enriched intelligence from Sentinel within Cyware Intel Exchange to validate indicators, accelerate investigations, and streamline workflows enabling security teams to act immediately.

Intelligence Enrichment and Ingest

Intelligence generated in Sentinel is automatically ingested into Cyware Intel Exchange for enrichment and validation, then disseminated to ISAC members or across enterprise hubs, strengthening collaboration across the broader security community.

CYWARE + Microsoft Defender

Operationalize Threat Intelligence at Scale

Ingest Defender threat intelligence feeds into Cyware Intel Exchange, enrich them automatically, and perform indicator checks to improve fidelity, reduce analyst false positives, and accelerate triage.

Threat Hunting

Run advanced hunting queries on Microsoft Defender for Endpoint using Cyware Intel Exchange and feed results into ticketing or response workflows, enabling proactive detection of emerging threats.

Indicator Actioning and Blocking

Automatically block malicious indicators on MDE agent nodes or contain affected machines based on Cyware Intel Exchange intelligence and response playbooks, providing real-time endpoint protection.

Step Into the Future of Unified Threat Intelligence Operations and Collective Defense with the Collaborative Power of Cyware and Microsoft.

Book Your Demo Today!

For more information:

111 Town Square Palace Suite 1203 #4 Jersey City, NJ 07310   cyware.com | sales@cyware.com

CYWARE™