CYWARE™

DATASHEET

Threat Defender Collaboration

Go Beyond Threat Intelligence Sharing. Share and Receive SIEM Rules, YARA Rules, Sigma Rules, MITRE ATT&CK Data, Automated Response Playbooks, and More....

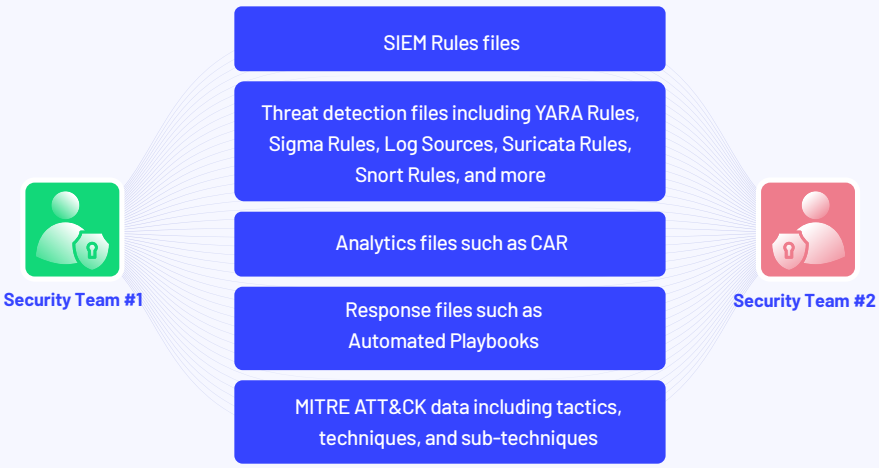
The Threat Defender Library is a new capability offered within Cyware's threat advisory sharing and security collaboration platform Collaborate that functions as an exclusive repository for security teams to store, collaborate, and share threat detection files, threat response automation rules, and threat analytics files between organizations.

With threat defender collaboration, siloed security teams can quickly respond to organization-specific threats by adding value to their existing threat hunting and threat detection workflows.

Security teams can build their own threat defender repository using Cyware's out-of-the-box templates, visualize critical metrics, and share it with other security teams in real time through Cyware's industry-popular automated alert sharing capability.

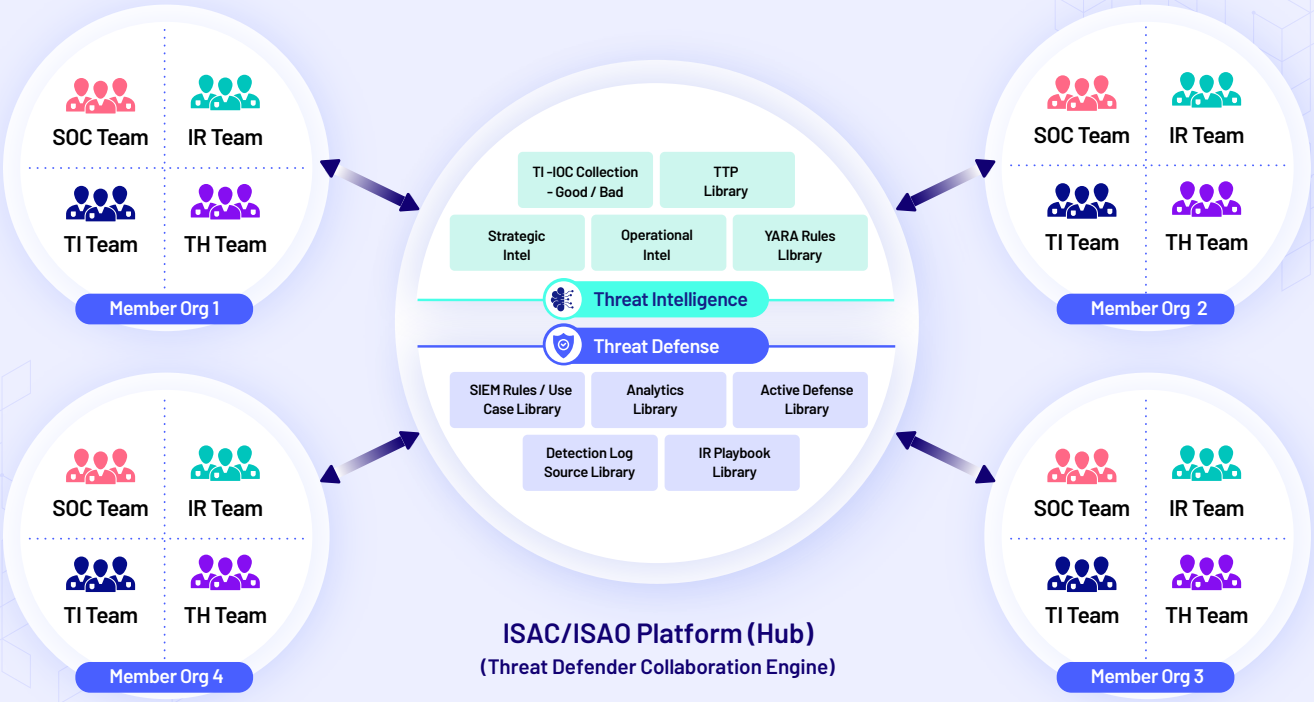
The new technology offering by Cyware will eliminate silos between security operations center (SOC), incident response, threat hunting, and threat intelligence teams within organizations and foster collaborative synergies against advanced cyber threats at sectoral (ISAC-to-Member) and cross-sectoral (ISAC-to-ISAC) industry levels.

What all you can share and receive from other security teams



Threat Defender Library Benefits

- Gain visibility into proven threat detection and mitigation strategies put in place by security teams from other organizations and industry sectors.
- Quickly respond to organization-specific threats by reusing the shared detection, analysis, and response files.
- Reduce time spent by analysts in researching and developing threat containment strategies.
- Mitigate common threats by actioning shared threat detection files such as SIEM Rules into deployed SIEM or XDR platforms.
- Increase threat hunting capabilities and significantly reduce MTTR and MTTD.
- Visualize a centralized mapping of threats and detection content against threat methods used by threat actors.



ISAC/ISAO Platform (Hub)
(Threat Defender Collaboration Engine)

Use Cases

Use Case 1	Threat defender collaboration between threat sharing (ISAC/ISAO) community members
Challenge	Siloed security teams from various organizations and industries create and deploy their own defense rules, which is time-consuming.
Solution	The threat defender library solves this challenge by enabling ISAC/ISAO members to deploy threat-defending mechanisms and files shared by other members. This drastically brings down the threat detection and mitigation time.

Use Case 2	Bi-directional and structured sharing of threat defender files
Challenge	Lack of scalability of threat defender operations due to unstructured storing and sharing of defender data and files in various formats such as emails, documents, corporate chats, etc.
Solution	The threat defender library solves this challenge by serving as a centralized, single window platform for security teams to create, store, and deploy threat defender data shared by their ISAC/ISAO hubs and member organizations

Use Case 3	End-to-end threat defense visibility and management
Challenge	Currently there is no platform that enables security teams to view and manage threat defense prevention practices and signatures
Solution	The threat defender library solves this challenge by serving as a central repository of ISAC/ISAO and member-shared threat defender content including threat indicators (IOCs), tactics, techniques and procedures (TTPs), etc. The library provides centralized visibility into all the defender content for each ISAC/ISAO member and allows them to visualise their defenses mapped to MITRE ATT&CK framework.

Cyware
111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310
855-MY-CYWARE
sales@cyware.com | cyware.com

CYWARE™