CTA Membership Admission Requirements

MEMBERSHIP REQUIREMENTS

A CTA member must be:

- Able to share and to receive technical cybersecurity information.
- A legal entity.
- Eligible to conduct business in the U.S. or with U.S. entities.
- Free from undue risk and influence due to government affiliations (other than customer relationships).
- In compliance with U.S. Export Administration Regulations, International Traffic in Arms Regulations, and other U.S. export restrictions, to the extent applicable.
- Able to protect CTA and its members' information.

MEMBERSHIP TIERS AND DUES

CTA membership dues are based on the chosen membership level (Charter, Affiliate, Contributing) and the member's global annual revenue (GAR).

CTA has three member categories: Contributing, Affiliate, and Charter.

Each requires a different level of commitment in return for a greater say in how the organization is managed and run.

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.

TECHNICAL REQUIREMENTS

- All members are required to **share a minimum amount of cyber threat intelligence**.
- Members must **automate submissions** to CTA's sharing platform (Magellan) to meet our sharing requirements.
- Members must make submissions in the **STIX 2.0 format**.
- All submissions are **scored and assigned points** based on CTA's proprietary scoring algorithm.
- All submissions must **include an indicator and context**.

Indicator Sharing:

Members are required to submit Indicators of Compromise (e.g., Malware File, IP address, Domain, URL, Port, Mutex, etc.)

Required Context:

Members must provide certain context with every submission. Required context includes kill chain phase, first seen, last seen, and number of times the indicator was sighted.

Optional Additional Context:

Other context is optional but improves the quality of the overall submission and helps members meet automated sharing requirements. This optional context includes but is not limited to malware name, type, and/or sample, MITRE ATT&CK technique, threat actor, and the sector and/or country of the targeted entity.