CYBER THREAT ALLIANCE

HOW WE CREATE UNIQUE VALUE FOR OUR MEMBERS

CTA member companies vary widely in terms of size, geographic coverage, and industry vertical. We recognize this diversity as a strength, as it allows our membership to bring together different pieces of intelligence and understand the broader picture.
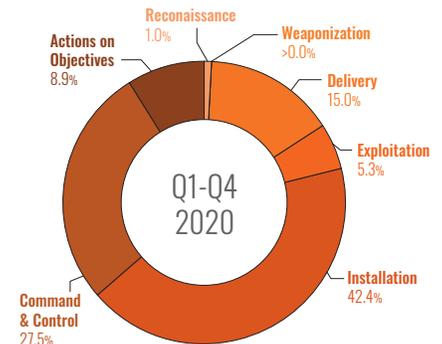
CTA has various membership tiers and partnership opportunities to ensure that we create value across the diverse business models of current and prospective members. Although we require a minimum amount of automated sharing to support CTA's mission, our mix of sharing, collaboration, marketing, and networking activities allows members to control how they derive value from their involvement with CTA.

AUTOMATED SHARING

Members use our automated platform to share curated and actionable threat intelligence that can be deployed to customers in near-real time. CTA members share around 6.5 million observables per month. Submissions also include contextual information, such as first- and last-seen, kill chain phase, ATT&CK TTPs, and affected industry, which allows our members to better understand the threat and action it for their customers. Threat data is drawn from endpoints, network devices, IoT devices, and ICS. We use a transparent and intuitive scoring algorithm to verify that members meet a minimum sharing requirement and to incentivize sharing of specific data types. Even our largest members report receiving 'new-to-them' threat intelligence data through CTA.

Reconaissance 1.0%
Weaponization >0.0%
Actions on Objectives 8.9%
Delivery 15.0%
Exploitation 5.3%
Q1-Q4 2020
Installation 42.4%
Command & Control 27.5%

OUR AUTOMATED SHARING IMPROVES VISIBILITY UP AND DOWN THE KILLCHAIN

HUMAN-SPEED SHARING

CTA members routinely discuss emergent threats and share blogs or research prior to publication to maximize awareness and better protect their customers. CTA also brings together members' threat researchers every other week to discuss trends, highlight upcoming work, and receive briefings. By serving as a trusted information and coordination hub for the cybersecurity industry, CTA is able to support operational collaboration around significant cyber incidents. During such crises, CTA and its members use shared intelligence to identify defensive actions that can reduce the overall effectiveness of malicious actors' tools and infrastructure.

AVERAGE WEEKLY EARLY SHARES FROM CYBER THREAT ALLIANCE MEMBERS

3-5

COLLABORATIVE IMPACT

- **Threat Disruption** — CTA runs working groups focused on specific topics, such as securing major events (elections, Olympics, etc.) and addressing high-profile and emerging threats
- **Thought Leadership** — CTA amplifies the research of our members, and works as an industry-wide rolodex for when members need more information about a threat, adversary, or pattern of activity
- **Industry Influence** — CTA participates in various cross-industry efforts and creates event participation opportunities for members, such as via our webinar series and CTA-sponsored conferences
- **Policy Engagement** — CTA provides a forum to discuss policy affecting the cybersecurity industry and can speak for ther cybersecurity provider community as a collective whole
- **Partnerships** — CTA has productive relationships with ISACs, CERTs, and other non-profit organizations

CYBER THREAT ALLIANCE JOINT ANALYSIS: SECURING EDGE DEVICES

MORE SUNLIGHT, FEWER SHADOWS
Guidelines For Establishing & Strengthening Government Vulnerability Disclosure Policies

Partnership against Cybercrime
INSIGHT REPORT
NOVEMBER 2020

2020 SUMMER OLYMPICS THREAT ASSESSMENT
TOKYO 2020