



THREAT INTELLIGENCE SHARING: WHAT IT MEANS FOR YOUR BUSINESS

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 cyber threat information sharing among member companies and organizations in the cybersecurity field. We share information through both **automated** and **analytic** channels.

WHAT CAN YOU DO WITH CTA'S SHARED THREAT INTELLIGENCE?

AUTOMATED SHARING

CTA members enjoy a broad license to repurpose threat intelligence data shared through our automated platform, Magellan. As a member, your organization can incorporate data received through CTA into products or services. However, products or services that utilize CTA data must simultaneously use other, non-CTA sources for a majority of the threat intelligence data that they drawn upon.

ANALYTIC SHARING

Analytic sharing generates deeper insights, creates trust and connections between members, and enables early warnings about upcoming publications through CTA's Early Sharing program. CTA members can use the insights that they receive through this program to prepare or implement improved protections ahead of time, as permitted under the TLP designated by the CTA member sharing the information (e.g., White, Amber, Red).

WHAT DOES CTA SHARE?

CTA shares a total of **ten different types** of cyber threat intelligence (CTI) across **four levels**:

Technical | Tactical | Operational | Strategic



Threat Researchers

Access a greater volume of more varied data to validate findings and rule out false positives, and dig into threats targeting particular sectors or regions.

Make use of shared data on specific threats to advance disruption efforts, including through topic-focused working groups, which can leverage separate instances of the Magellan platform.



Threat Hunters + SOC's

Leverage the reliability and accompanying context of CTA indicator data for both machine-based and manual scrutiny of emerging threats to supplement existing data and connect the dots around adversarial activity

Gain broader visibility into adversary behavior and how it is evolving through the inclusion of ATT&CK TTPs in shared data.



Product Owners

Incorporate CTA's machine-readable shared data into delivering stronger protections for customers across the board.

Access malicious file samples, domain names, URLs, and other observables that can be automatically cross-referenced with SIEM data from inside the enterprise to improve targeted protections.



Executives + C-Suite

Gain early access to threat reports, strategic information, or situational warnings from private sector peers and public sector partners

Provide executives with greater and more timely visibility into emerging threats uncovered by other CTA members and partners. No vendor has full visibility into the threat landscape, so every member brings something unique to the table.