Automated Indicator Sharing

OVERVIEW

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA's) free Automated Indicator Sharing (AIS) program enables organizations to share and receive machine-readable cyber threat indicators (CTIs) and defensive measures (DMs) in real time to monitor and defend their networks against known threats that are relevant to AIS participants.

WHY PARTICIPATE IN AIS?

By participating in AIS, organizations can send and receive CTIs/DMs with other organizations and can be on the lookout for similar activity to proactively defend their network. This allows organizations to benefit from the collective knowledge of participant organizations. AIS also offers anonymity, as well as liability, and privacy protections to encourage the submission of CTIs/DMs related to successful or attempted compromises.

THE CYBERSECURITY INFORMATION SHARING ACT OF 2015

AIS is available through CISA's Cybersecurity Division and CISA Central which are designated as the hub for the sharing of CTIs/DMs between the federal government and private sector by the Cybersecurity Information Sharing Act of 2015. This law grants liability protection, privacy protections, and other protections to organizations that share CTIs/DMs through AIS in accordance with the Act's requirements. As mandated by the Cybersecurity Information Sharing Act of 2015, DHS certified the operation of AIS in March 2016. The goal is to share tactical CTIs/DMs through AIS broadly among the public and private sector, enabling everyone to be better protected against cyberattacks.

LIABILITY PROTECTION

Liability protection is granted to organizations for sharing through AIS if the sharing of CTIs/DMs is done in accordance with the Cybersecurity Information Sharing Act of 2015. Liability protection applies to:

- Non-federal entities sharing with other non-federal entities;
- Non-federal organizations sharing with information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs);
- Non-federal entities sharing with CISA and other federal agencies through AIS.[1]

Federal organizations do not receive liability protection when sharing with one another, but some aspects of the Cybersecurity Information Sharing Act of 2015 apply (e.g. privacy requirements when sharing CTIs).

PRIVACY PROTECTIONS

CISA has taken careful measures to ensure appropriate privacy and civil liberties protections are fully implemented in AIS. CISA has published a privacy impact assessment of AIS found on https://www.cisa.gov/automated-indicator-sharing-ais.

[1] For more information regarding liability protection under the Cybersecurity Information Sharing Act of 2015 and other protections that may apply, see the Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015, available at https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation.

To ensure that personally identifiable information (PII) is protected, AIS has processes which:

- Perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat;
- Incorporate elements of human review on select fields of certain CTIs/DMs to ensure that automated processes are functioning appropriately;
- Minimize the amount of data included in CTIs/DMs to the information that is directly related to a cyber threat;
- Retain only information needed to address cyber threats;
- Ensure any information collected is used only for network defense or limited law enforcement purposes.

HOW AIS WORKS

AIS leverages the Structured Threat Information Expression (STIX) standard to represent CTIs/DMs and the Trusted Automated Exchange of Intelligence Information (TAXII) standard for machine-to-machine communication. AIS participants connect to AIS with a STIX/TAXII capability (which can be built or bought from commercial vendors) to allow them to exchange CTIs/DMs.

HOW TO PARTICIPATE IN AIS

The federal government is actively sharing CTIs/DMs through AIS, but we always need more organizations to join—both to receive and share CTIs/DMs! To connect, please complete the following steps:

1. Contact cyberservices@cisa.dhs.gov (engagement information) or taxiiadmins@us-cert.gov (technical assistance during onboarding).
2. Agree to a short Terms of Use for non-federal organizations or the Multilateral Information Sharing Agreement (MISA) for federal organizations.
3. Get a STIX/TAXII capability: use an open source TAXII client, provided by DHS or others in the community (e.g., ISACs, ISAOs), or obtain access via a commercial solution.
4. Purchase a PKI certificate from a Federal Bridge Certificate Authority.
5. Sign an Interconnection Security Agreement and provide your IP address to CISA.

For a list of vendors, ISACs, and ISAOs that participate and further distribute CTIs/DMs to their downstream customers, please visit https://www.cisa.gov/automated-indicator-sharing-ais. Other important documentation is also posted there.