IACD

Integrated Adaptive Cyber Defense

Trends in Technology: Threat Intelligence Platforms

Published February 2019

Threat Intelligence Platforms or TIPs, ingest, correlate, and share threat information for multiple purposes including: threat analysis, risk prioritization, and incident detection activities. TIPs enable rapid information aggregation and sharing, assisting analysts by bringing large collections of data together to form a more comprehensive illustration of the dataset. TIPs also facilitate sharing within the platform and beyond to benefit the entire cybersecurity community. This handout provides you with a quick analysis of some of the common characteristics and operationally critical features of this rapidly maturing technology. Whether you're interested in purchasing TIPs products or just trying to keep up with the latest trends in technology, take a few minutes to see what many of them can offer.

Automation

TIPs are increasing the amount of automation they can provide to support threat analysis processes and network defense activities. Certain TIPs have started to implement orchestration capabilities into their systems. Currently, the most common automation feature is the ability to set up rules to enrich or process the data further. Another common feature is the ability to share intelligence in an automated fashion.

Collaboration

TIPs facilitate the creation and organization of groups within their platform in which only the users in certain groups have access to the threat intelligence data. They also support Role Based Access Control (RBAC) to ensure only the proper users have the ability to configure or change the feed.

Community Perspective

TIPs provide users the option to share their information with a wider trusted group in an anonymized or named fashion. This allows users to check if their indicators have been seen by other users, which builds confidence in the accuracy of the indicator's score.

Data Integration

TIPs are designed to ingest and correlate threat information from multiple sources in multiple formats. All of these platforms perform some normalization of the different datasets to enable automated processing, analysis, and visualization.

Analyst Dashboard

This is the graphical user interface that serves as the homepage for the Analyst to interact with the product. This feature is commonly customizable; it displays graphics for metrics, recent threats, an overview of the TIP's process, etc. Easy-to-use visualization capabilities are a major component of TIPs and the analyst dashboards often have links or buttons to quickly visualize additional information or context.

Data Storage

TIPs are designed with the assumption that the user will have access to any/all of the data ingested, created, and/or shared via the platform at any time. These platforms often serve as a system of record and this information is usually available through a designated query language or API.

On-Premises, Off-Premises

While many TIPs offer on-premise services (that may or may not be connected to other users of the platform), they encourage users to move towards their off-premises (often cloud-based) construct, as storing data and capturing user knowledge in one location fosters the usage of community perspective services.

Prioritization

TIPs generate and apply their own score to every indicator posted to their service, which provides means to prioritize indicators according to their importance and/or maliciousness.

http:// https://iacdautomate.org @IACD_automate https://www.linkedin.com/groups/8608114 icd@jhuapl.edu

Robust APIs

TIPs vary in the breadth and depth of their documentation; however, the user can do more with the TIP's API than they can with their GUI, thus demonstrating how TIPs are designed to be orchestrated rather than orchestrate. These interactions require an authentication method which varies amongst TIPs.

Markings ✓

Many TIPs can handle standard markings, such as Traffic Light Protocol, but are currently unable to handle custom markings, sometimes stripping them off of the indicator when they initially process it. By doing so, this creates a security issue as indicators without their markings can easily be mishandled.

Proprietary Data Models

TIPs often have their own data model and their own proprietary way to interact with their tool. This creates an issue when data is translated repeatedly between STIX and their own proprietary form, as information can easily be lost or misinterpreted. Some TIPs do however retain the original STIX formatted objects in their data stores, which can be used/referred to by users. Scoring methods are also often proprietary, which reduces the user's trust in the score.

Client and Server

As a user of the TIP, you have the ability to be both a producer and a consumer of threat intelligence. The user has a dashboard, an API, and the ability to input and export data with STIX/TAXII.