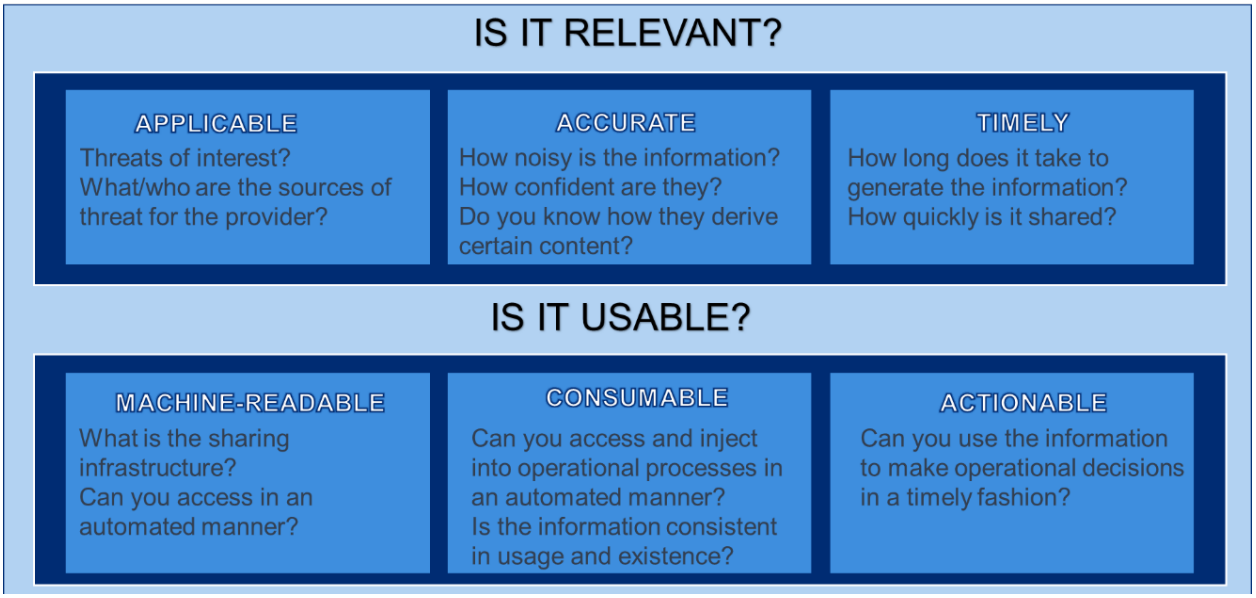
ASSESSING THE POTENTIAL VALUE OF CYBER THREAT INTELLIGENCE (CTI) FEEDS

Usability and Relevance for CTI

Kimberly K. Watson

There is an ever-expanding market of CTI feeds and providers. Most organizations have invested in, or are going to be investing in, these feeds with the promise of improved situational awareness, enhanced network defense capabilities, and data to inform prioritization of resources. How can an organization assess a product, service or feed and associated cost to ascertain what solution best aligns with the organization's requirements?



There are two areas of consideration to assess the potential value of a CTI feed: relevance and usability. However, most organizations only focus on relevance. While determining if an offering is relevant is important, it is not enough. The organization / customer / consumer also needs to make sure the information is usable and applicable in their environment; that it is actionable and can be used to drive the operational

processes and decisions in a timely manner with minimal impact to local resources. This paper provides definitions and operational considerations for assessing the potential value of CTI feeds.

Relevant

Relevance is a key factor in determining how much value a CTI feed can provide. It essentially answers the question: “Does the information focus on what I need to make informed and timely risk decisions regarding threats to my operations, assets, and organization?”

Applicable

Definition: The data feeds collect and share information directly related to the threats and risks of interest to the organization.

Considerations: Applicable is dependent on the organization. It is directly tied to the mission, the types of assets, the threat posture, as well as regulatory requirements. One aspect of Applicable that is easily overlooked are the sources of data used by the producer of the CTI feed. If the initial data comes from organizations that are in the same sector or have similar operational environments, then it is more likely to produce CTI that is applicable than those that use multiple sources that do not share mission, asset, or risk considerations.

Accurate

Definition: A level of confidence or correctness has been associated with the information provided in relation to a documented community standard.

Considerations: Accurate is dependent on the community standards and/or best practices used by the producer of the information. It is important to understand what the information being provided means, how it is curated, and how much confidence is applied to the resulting data sets. An organization needs to make sure that the information they get is accurate enough for how they intend to use it, as some processes are very sensitive to incorrect information or inference. It is also important to understand any logic used to create a piece of information (e.g., confidence score, severity) to determine how to appropriately use that information in local operations.

Timely

Definition: The information is providing insight into threats in time for the organization to make relevant risk decisions.

Considerations: Timely is dependent on the processes of both the provider and the organization. It is important to understand the timeline of when the producer learns about a potential threat as well as the investigation, curation, and sharing of processes.

Once that timeline is understood, the organization needs to consider if the information is being provided in time to make the desired risk decisions. Information for use by a Security Operations Center (SOC) to block malware has a very different timeliness requirement than information needed to build a strategic view of threat for investment decisions for protective technologies.

Usable

Usability is critical to determining how much value can be realized from a CTI feed, particularly when being applied to operational activities beyond traditional threat analysis. These activities have a defined operational tempo and decision criteria, so there needs to be an assessment of whether the data contained in the information can be made available to operational processes in a manner that supports timely and appropriate risk decisions. This focus area answers the question: “Can I access, process, and use the information to implement a timely mitigation to a valid threat in alignment with local policy?”

Machine-Readable

Definition: The data is provided in a structured format that can be processed in an automated manner.

Considerations: Machine-readable is dependent on the systems exchanging the data. It is important to know what formats the provider supports for both content and delivery, and ensure that the consuming organization has the capability to use the sharing infrastructure in an automated manner. At one level, there is the issue of format (e.g., JSON, XML). At another level, there is an issue of data structure, i.e., do you have a piece of software that implements the same version of the standard such that you can parse out the formatted data?

Consumable

Definition: The data can be accessed and converted into information that is used by operational processes in a timely manner.

Considerations: Consumable is dependent on the system and the processes that use the information. How do they access data? Can data be consistently derived from the information? What is required by the processes being fed by this information? A large part of consumable is timeliness, i.e., can the data be received, processed, and used within the period of time in which it has operational meaning? This is where sharing infrastructure / accessibility considerations are identified, and also where inconsistency in the data becomes an issue. For the sake of CTI that is Indicator of Compromise (IOC) based and meant to be used by network defenders, being consumable implies that the

access and conversion processes as well as injection into operational processes all be performed in an automated manner.

Actionable

Definition: The data can be converted into information that is used directly by decision-making processes within the timeframe that making the decision has value.

Consideration: Actionable is dependent on the decision-making processes that use the information. What are the decisions that you want to make? This includes not just content and timeliness, but also related characteristics that make the information usable by those processes in the timeframe needed for the decision. Other characteristics are things like confidence for threat analysis decisions and relevance for network defense decisions. The existence of these characteristics needs to be either inherent in the existence of the information or explicitly included in / easily derived from the content itself. In the first case, transparency is critical for acceptance / usage of the shared information. In the second case, it is consistent use of information to provide context that is critical. With respect to IOCs being used to drive network defense actions, actionable implies two things: that the conversion process and injection can be done in an automated manner, and that the resulting information meets characteristics required by the decision-making process.

Acknowledgement

This material is based upon work supported by the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency under Grant Award Number DHS-19-CISA-128-SLT-001 (State, Local, Tribal, and Territorial Indicators of Compromise Automation Pilot).

Disclaimer

The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.

✉ Kimberly Watson
Kimberly.Watson@jhuapl.edu