Cybersecurity Automation and Threat Intelligence Sharing Best Practices

Feb. 2021

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

UNDERSTANDING SERVICE MODELS FOR CYBER THREAT INTELLIGENCE (CTI)

Intelligence, Enrichment, and Brokering as a Service

Kimberly K. Watson

There are many CTI products and services on the market today. While the type of content is similar, the service models being applied are vastly different. From an operational standpoint, the value provided by the different service models varies significantly and is directly associated with the consumer and their intended usage of the CTI.

Service Model	Service Intent	Core Content	Operational Value
Intelligence as a Service	To get an organization's CTI out to a large and diverse set of consumers (1->Many)	Unique CTI	Depending on the source, the CTI could be more applicable, trusted, timely, or accurate.
Enrichment as a Service	To take multiple sources of CTI and put it in context for use by a particular consumer type (Many->1)	Contextualized CTI	CTI that is designed to support sense- and decision-making activities.
Brokering as a Service	To take multiple sources of CTI and make it all available to a large and diverse set of consumers (Many->Many)	Normalized CTI	A single infrastructure for receiving CTI. A single data structure and point of access for ingestion and processing.

Intelligence as a Service

An "Intelligence as a Service" model provides organizations a CTI feed curated from information collected or discovered as part of normal business operations. The organization is the source of all the information in the feed, and can make verifiable claims about accuracy, timeliness, and type of content based on well-defined industry standards. They can also guarantee consistency in certain fields (e.g., confidence score) as well as provide transparency into how values are generated.

The operational value of “Intelligence as a Service” feeds is directly related to a set of factors including, but not limited to:

- Uniqueness and applicability of the CTI
- Timeliness of processes to collect, derive, and share the CTI
- Credibility, competency, and transparency of the organization providing the CTI

Enrichment as a Service

The most common model associated with CTI sharing is the “Enrichment as a Service” model. An “Enrichment as a Service” provider consumes multiple feeds from other sources (to include their customers), and then applies some business logic to produce a CTI feed that is designed to serve a particular community or consumer type. Examples of common business logic include: threat analysis, filtering, scoring, cross-correlation, and context development.

The point of enrichment is to add context and support operational sense- or decision-making. Therefore, an “Enrichment as a Service” feed is only valuable if it is consumable and actionable[1] by the operational element using it. This implies that the feed can be accessed and converted into information that is used by operational processes in a timely manner. Another consideration is whether the feed can be converted into information that is used directly by decision-making processes within the timeframe such that making the decision has value. Using “Enrichment as a Service” feeds for decision-making support requires that the business logic applied to the CTI by the producer either matches or can be directly mapped to that of the consuming organization. If the logic is not provided, or if it does not align with local policies, the feed can still be valuable if it contains all the information required to make an appropriate local decision.

Brokering as a Service

“Brokering as a Service” is another common CTI sharing model in which the producer ingests multiple feeds, maps the content to a single data structure or model, and then shares all the content with consumers that have a legal right to the information. The main purpose of a broker is to normalize all the information from multiple sources to make it easier for organizations to ingest, visualize, and perform analytics on large sets of CTI.

The operational value of a “Brokering as a Service” feed is directly related to the consistency of the information provided by the sources and accessibility of the resultant feed. If the sources use different definitions or logic for common data fields, it is very hard for the broker to accurately map these different sources to a single data model.

[1] Watson, K., “Assessing the potential value of cyber threat intelligence (CTI) feeds”, Dec 2020.

While humans may be able to correct for underlying inconsistencies, automation usually cannot, which limits the usability of the feed to drive time-sensitive operations. Another issue is the inclusion of special content used by only one source that is not easily mapped to an element of the existing data structure. This results in the loss or misrepresentation of information being brokered which limits the scope of content that can be used for correlation or advanced analytics. It is equally important that local data can be easily mapped to or correlated with the broker’s data model, and that the API for importing and exporting data is accessible in an automated manner.

Conclusion

Organizations considering participation in a CTI sharing community or subscribing to CTI feeds need to understand the service model being used by the provider. Different service models provide different types of value, and an organization needs to define the operational use cases for the CTI to determine the operational value of the proposed investment.

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.