Evaluating the Value of Security Intelligence Feeds with Silent Push

silentpush.com/blog/evaluating-the-value-of-security-feeds-with-silent-push

September 29, 2021

Sep 29

Written By Seth Hamlin

The value of cyber security, threat intelligence feeds can't be overstated. However, like all security measures, not all cyber threat intelligence feeds are created equal. So what are some of the differences between a good and a great security feed?

There are of course a variety of factors that play into the value of any particular security feed. Some common considerations are relevancy and usability.

Unmeasurable Factors in Cyber Threat Intelligence Feeds

Generally speaking, a security feed that provides highly relevant data is providing data that is closely related to the target business or organization. Nowadays, many threats are targeted at specific businesses, which makes relevancy a critical factor in evaluating

feeds.

Usability refers to how likely it is that information supplied by the security feed can lead to decisions that improve security. One of the end goals of a security feed is to allow for decisions that improve security policy making. If feed items only contain domains, IPs or hashes without any reasoning or clues as to why they are there, then they are not so useful. Each item needs to come with clues as to why it is suspicious and some information about how the feed is compiled in the first place so you know what you are looking at. Most importantly, this context will help you know how to use the information.

These factors are rare enough. One of the problems is, any given company may pay for a large number of security feeds. These feeds are quite expensive and may supply data that is repetitive. In the worst cases, one feed may simply be copying another. However, security feed analysts at the company may never know.

Expanding upon that, it's also helpful to know which feeds are the first to share any potentially useful information. If we have five security feeds that all detected the same potential risk, we want to know which detected it first and which last. In this way, one can identify which feeds are the most valuable and which could be cut.

Evaluating Cyber Threat Intelligence Feeds with Silent Push

Silent Push provides two unique metrics to address the above issues to identify the best cyber threat intelligence feeds.

One of these metrics is called **overlapping percentage**. This refers to the proportion of indicators (IoCs) on that feed that are also seen on other feeds. Of course, a feed that provides unique data, data that isn't seen on other feeds, can provide valuable insights.

Another percentage-based metric is **originality percentage**. Originality percentage means the proportion of indicators on any particular feed which were first shared by that feed. A feed that provides a large amount of original intelligence is a valuable asset to a business or organization.

To determine the value of a CTI feed against another, or many others, these two metrics are quite useful. Relevancy and usability are more closely connected to the information within a singular feed. But if a company is paying for many feeds, it's possible that all of them can score high on relevancy and usability.

By employing these two additional metrics, unique to Silent Push, companies can save money and time by easily determining which feeds are the most valuable.

Value can translate into more than just spending less on repetitious security feeds. By identifying which feeds supply the best information the fastest, it may also be possible to react to targeted threats before they cause any damage. The concept of proactive threat detection, rather than reactive, is core to the Silent Push mission.

There's an interesting paper here on ways on how some academics evaluated security intelligence feeds and some of their results.

Seth Hamlin