The Practical Implications of Collecting, Analyzing, Evaluating Threat Intelligence Data

The Center for Protection of the National Infrastructure (CPNI) and CERT-UK recently sponsored a white paper called Threat Intelligence: Collecting, Analyzing, Evaluating. The paper discusses the need for ensuring that intelligence collected be relevant for all security stakeholders in your organization. There is a myriad of threat intelligence providers each with their own threat data specialty that produce the data in a variety of formats. This paper discusses a technical approach for making threat data fit their subtype classification model in figure 1.

The following definitions are supplied in the white paper for each threat intelligence subtype:

- **Strategic Threat Intelligence –**
  "...is unlikely to be technical and can cover such things as the financial impact of cyber activity, attack trends, and areas that might impact on high-level business decisions." This information would be considered to be business vertical relevant.

- **Operational Threat Intelligence –**
  "...is information about specific impending attacks against the organization and is initially consumed by higher-level security staff, such as security managers or heads of incident response".

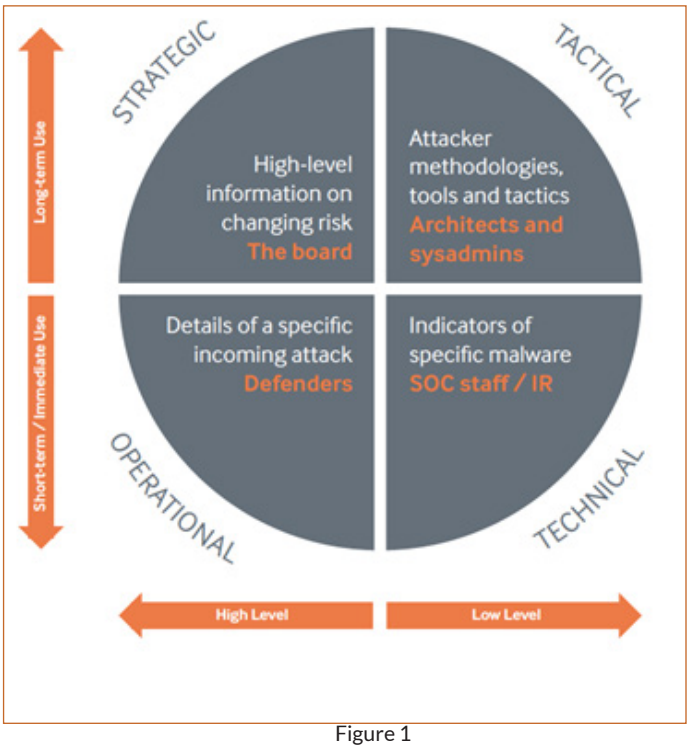

Figure 1

- **Tactical Threat Intelligence –**
  "...is often referred to as Tactics, Techniques, and Procedures (TTPs) and is information about how threat actors are conducting attacks."

- **Technical Threat Intelligence –**
  "...is information (or, more often, data) that is normally consumed through technical means.

Threat Intelligence is now its own big data problem making classification into the sub-categories listed in the white paper very difficult. Big data is defined by the 3-Vs of volume, velocity, and variety. Anomali is currently tracking tens of millions of active indicators of compromise (IOCs) in threat data. This number has accumulated over just two years. The data comes in a variety of formats. With adversaries creating millions of domains that use domain generation algorithms to stay one step ahead of botnet detection, the velocity of change is easily identified. Curation of threat data by organizations into the suggested subtypes can't be done manually.

Recommendations

A threat intelligence platform needs to be the starting point for initial curation of the threat data. It will help with normalization and deduplication of the data, come with an initial set of feeds based on open source information, and vetted trusted circles your organization can join or create. The challenge of **making threat data strategic** starts with identifying the threat data feeds with the most relevance for your organization. The threat intelligence platform vendor can be somewhat helpful with this based on past history but using the vetted trusted circles to simply ask other organizations in your business vertical is better. What you often find out is what organizations in your business vertical are seeing and how they are dealing with these threats. This information can be delivered at the Board of Directors and CEO level of the organization.

Making threat intelligence tactical as defined in the white paper is often accomplished in the threat intelligence platform through data exploration techniques. For example, starting with one domain indicator, you can:

- Determine all the IP addresses associated with the domain
- Review the email address of the domain registration
- Find other domains registered to the attacker and identify associated IP addresses and
- Take defensive action against the potential attacker

The operational value of threat intelligence should come from the threat intelligence platform. Information about the campaign, where the attacker may be based, and other information about attacker techniques should be provided as a matter of course by the threat intelligence platform. These details should help you recognize similar attacks by the same attacker.

Technical usage of the of the threat intelligence data is perhaps the hardest thing to do. The threat intelligence big data problem places an arbitrary ceiling on the amount of data that can be correlated with log data in security information and event management systems (SIEM). The SIEM was not designed to look at tens of millions of IOCs and correlate them with massive amounts of security relevant data. Further, many companies don't keep data on-line and available for correlation long enough to look back past the 200-day attacker dwell time window outlined in may data breach reports. Threat intelligence platform purchasing decisions should take into consideration the organizational and operational relevance of IOCs being provided in the threat intelligence platform. New threat intelligence platforms having the capability to pre-analyze your log data for potential IOCs, match these to IOCs in threat data and return only the IOCs that are relevant at a given moment should be at the top of your list. These automated solutions reduce IOCs from tens of millions to the few hundred that might actually be useful.

Summary

The threat intelligence platform is the only way to be able to tackle this new big data problem and quickly and easily place threat intelligence into the sub-categories outlined in the whitepaper. However, the value of relevance is what makes threat intelligence data tactically, technically and operationally useful for proving strategic value to your organization.

ANOMALI™

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1.844.4.THREATS | info@anomali.com | www.anomali.com