Understanding the Threat Intelligence Lifecycle

BY JAMES PALAZZOLO

(http://darkmatters.norsecorp.com/author/jpalazzolo/)

()

Everyone is interested in Threat Intelligence (TI). There is a race to the top of the mountain with regards to providing 'Intelligence' on the 'latest threats'; but, what does that really mean for information consumers?

Firstly, let's look at the term 'Intelligence'. For most individuals the term Intelligence has several meanings ranging from covert operations to information gathering. However, very little time is actually spent on the Intelligence Lifecycle.

Understanding the lifecycle and some key framework concepts of Intelligence will help

people understand where TI really enters into Intelligence; and how the basics can be leveraged to derive value added information into the organization.

The Intelligence Lifecycle

Excluding the scope of Cover Operations and Counter Intelligence one of the key missions of an Intelligence program is to prepare the battle space. However, this article is not working within a military construct so for the contextual use of the rest of the article the battle space will be the organization.

From a technical perspective preparing the organization requires a mature asset and data management program. From this perspective there is no one-size-fits-all solution to asset and data management.

For those who are just beginning there are several resources available on the Internet to help organizations get started. Furthermore, there is no need to gather TI if asset management in not addressed as much of the TI will probably pertain to assets owned by the organization.

Once assets have been identified, classified, and entered into a management lifecycle an organization can begin to ask the right questions. This is the consumer request for information.

Some example questions may be: What threats are posed against Java resources, or are there relevant threats currently attacking other Windows based infrastructures? The question initiates the Intelligence Lifecycle: Collect, Analyze, and Disseminate.

Low Budget Entry Points

So now that we have a very basic concept of Intelligence where do we begin collecting this information?

For organizations wishing to do low budget Proof of Concepts or organizations that do not have the financial resources to developing robust Intelligence capabilities the two best places to start are in the domains of Human Intelligence (HUMINT) and Open Source Intelligence (OSINT).

These two terms are some of the most powerful and cost effective terms to learn from a collection standpoint.

HUMINT is comprised of human interactions. This can be anything from fellow security professionals, relationships with security vendors, local law enforcement, Social Media et al.

Developing human relationships with regards to on the ground information can be more valuable than any high tech platform. For example: The creation of a Twitter account that follows such things as hacktivist groups and malware developer communities can reveal large amounts of information.

However, like any other collection effort it will be an effort of labor to manage, maintain,

and sift through the vast amount of inbound information.

OSINT is the other low cost effective way to collect Intelligence. Always remember that Google is your friend. Simply typing in search terms like 'threats to java' or 'latest windows hacks' can reveal countless pages of information.

Furthermore, OSINT comprises of things like vendor supplied threat reports, news wires, streaming video, or just about anything you can obtain legally. For example: companies like Verizon publish yearly threat reports that cover a wide range of topics.

The nice part about these types of reports is that the information is typically backed by some form of metric which can help with augmenting risk assessments conducted by the organization.

Medium to High Budget Entry Points

Many security vendors now come with their own form of Intelligence engines. These hardware and software solutions share detected threats with each other to enhance the overall effectiveness of the solution.

As an example, many products produced by a vendor may talk to a centralized system that publishes new threats to all of the other of the vendor's solutions. However, these solutions cost more than your free or low budget options.

This is not to say that medium to high budget entry points should not be considered. Often times in order to derive good TI a mix of both low and high budget options need to be implemented.

Tying It All Together

Threats, internal threats, external threats, relevant threats, hacker threats, malicious threats, advanced threats, common threats, threats, threats.....WHERE ARE THE THREATS!!!???

So, now that we have a very basic view of Intelligence and Threat Intelligence let's look at a scenario regarding a local government who is ramping up their Cyber Security program but needs Threat Intelligence information to determine next steps.

The first step the organization performs is to recognize and understand the Intelligence Lifecycle. Once management understands the input(s) and output(s) of their request their expectations of returns will be on par with the initiative.

The second step the organization performs is to mandate the work to a security analyst within the organization. Although there are dedicated vendors who can also provide this information from a cost perspective this local government has decides to use an internal resource.

Once given the mandate for a generalized Intelligence effort the security analyst begins

looking at relevant collection mechanisms.

The analyst determines that there are some technical capabilities for Intelligence collection, but with regards to specific TI the analyst turns to more open sources of information (i.e. the Verizon reports mentioned above).

After two weeks of analysis the analyst feels confident that they may proceed to disseminate their findings. In this example they have determined that hacktivism, web site hijacking, and DDoS attacks are the primary threats to the environment from an external perspective.

After the information has been disseminated to all relevant stakeholders follow up meetings are scheduled to continue the discussion but from a roadmap and remediation perspective.

YOU MIGHT ALSO LIKE:

NUMBER ONE ON MY TOP TEN LIST FOR SECURITY EXECUTIVES: HISTORY'S LESSONS (HTTP://DARKMATTERS.NORSECORP.COM/2014/10/23/NUMBER-ONE-ON-MY-TOP-TEN-LIST-FOR-SECURITY-EXECUTIVES-HISTORYS-LESSONS/)

NUMBER TWO ON MY TOP TEN LIST FOR SECURITY EXECUTIVES: REFORM (HTTP://DARKMATTERS.NORSECORP.COM/2014/10/30/NUMBER-TWO-ON-MY-TOP-TEN-LIST-FOR-SECURITY-EXECUTIVES-REFORM/)

ACTIVITY FROM CHINESE IP CONTINUES, HIGHLIGHTS ATTRIBUTION ISSUES (HTTP://DARKMATTERS.NORSECORP.COM/2014/09/11/ACTIVITY-FROM-CHINESE-IP-CONTINUES-HIGHLIGHTS-ATTRIBUTION-ISSUES/)

CLASS ACTION SUIT OVER CHS BREACH IS CALL TO ACTION
(HTTP://DARKMATTERS.NORSECORP.COM/2014/08/29/CLASS-ACTION-SUIT-OVER-CHS-BREACH-IS-CALL-TO-ACTION/)

James Palazzolo

James Palazzolo is a Cyber Security Researcher with a focus on Cyber Intelligence. He has a degree in Information Assurance from Eastern Michigan and is currently scheduled to complete his Graduate Degree in Cyber Intelligence by the end of 2016. James has also worked in security for Healthcare and in Local Governments.

▶ MORE POSTS (3)
(http://darkmatters.norsecorp.com/author/jpalazzolo/)

TOPICS: ANALYTICS, ENTERPRISE SECURITY, HUMINT, NETWORK SECURITY, OSINT, RISK MANAGEMENT, SECURITY SOLUTIONS, SECURITY STRATEGIES, THREAT INTELLIGENCE,