Integrate Threat Intelligence program into your daily security operations - Phase 2 - Collecting Intelligence

In order to get the most out of your threat intelligence program, quality and quantity of data must be collected and filtered. Below are some indications for analysing what should be collected and whatnot:

- Collect the right data according to stakeholder's requirements
    - stakeholders can be analysts, managers, C-level executives, IR team, VM team, DFIR team, etc.
- Map stakeholder's requirement of collecting data to your internal and external data sources
- An organisation needs to have proper tooling, resources and solutions to collect the right quality and quantity of data.
- An organisation needs to prioritise its goal in order to collect what type of data.
    - For, e.g. what threats/vuln/incidents/anomalies, they need to focus more.

Collection of data is the process of ingesting data from various below sources.

A couple of important data collection sources are:

- individual information (personal information)
- organisation/company information
- Domain/IP/URL/ information
- Business information
- Document leaks information
- Information from telegram and WhatsApp groups
- Information from threat search engines
- Information from the dark web
- Information from commercial solutions (Recorded future, RiskIQ, CrowdStrike, etc.)
- Information from IoC data feeds
- Information from social media
- Information from media files
- Information from counterintelligence feeds
- Information from internal company logs
- Information from external sources such as journals, blogs, forums, etc.

Intelligence collection depends on the major two criteria.

1) Commonness of an attack - In this criteria, the organisation needs to decide how often a particular threat/attack can occur to their organisation. Based on this information, they can also prepare a graph that can provide an indication whether that particular threat is increasing or decreasing over the period.

2) Impact of an attack - In this criteria, the organisation needs to decide how a particular threat which is increasing or decreasing can affect a company's critical services technically as well as financially. How it can disrupt services and how wide is the impact scale. Also, decide what type of information is on stack due to these attacks. How quickly an organisation can recover from this type of attacks.

Intelligence must be collected based on the above two criteria.

Below is the example of a couple of intelligence needs that an organisation can collect based on stakeholder's need and above two criteria:

- Zero-day attacks information
- Ransomware information
- Phishing information
- IoC information
- Website defacement information

- Insider activity
- Nation-state threat actors
- Hacktivists

A small example table can be prepared as follows in order to prioritise the intelligence collection strategy.

Threat Intelligence Priotisation Reuqirements											
Sr. No	Intelligence Requirement	Description	Probability	Increasing/Decreasing	Commonness	Business impact on processes	Data breach impact	Financial Impact	Recovery time	What to collect	For whom to collect
1	Phishing URLs	Phishign URLs that are impersonating organisation's legitimate website including content, look and information.	Often	Increasing	Once a month	None	Medium	Medium	High	URLs Domain IP	Incident response team
2	Zero-day attacks	Attacks that are not patched by official vendors or official vendors haven't produced fixes for these attacks.	Rare	None	Once a year	Medium	High	High	High	Threat actor name Platform details Tactic details Techniques detail Procedures details Origin country	Incident response team Forensics investigation team Vulnerability management team CISO, CTO
3	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.		
4	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.		
5	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.		
6	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.		

After prioritising intelligence collection needs and collecting data from various sources, it is time for the normalisation. According to Wikipedia, Normalization or standardisation refers to a process that makes something more normal or regular. Standardisation is a process of converting unstructured data into structured data. It is beneficial for everyone to have a single structured data so anyone can find anything easily from the collected data.

In threat intelligence, collection of data can be normalised into their standard accepted languages and procedures. Currently, in threat intelligence, there is no single accepted standard; however, basic four formats for the data structure is used within the industry, and they are **STIX, CybOX, OpenIOC,** and **TAXII.**

I am not going deep into these formats and their understanding as I want to focus on the topic I started. So here is the wonderful article written that explains STIX, CybOX and TAXII in detail.

https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/

Here is one the Youtube video that will explain the OpenIOC in detail.

Mainly threat intelligence collection sources are divided into three categories:

1) Internal - IDS, IPS, Proxy, Network, Firewalls, EDR, Anti-virus, Anti-malware, email, etc.

2) External - It covers open source feeds and information sharing channels that may include blogs, forums, IRC, etc.

3) Outsourced - It covers imported information from any commercial vendor.

Following is one of the best curated lists of excellent Threat Intelligence resources. Most of the resources listed there provide lists and/or APIs to obtain (hopefully) up-to-date information with regards to threats. Some consider these sources as threat intelligence, opinions differ, however. A certain amount of (domain- or business-specific) analysis is necessary to create true threat intelligence.

https://github.com/hslatman/awesome-threat-intelligence

There are major pros and cons of internal and external(outsourced) threat intelligence feeds. It can be described as follows:

#	Advantages	Disadvantages
Internal	Within the company, customisation becomes easy as the organisation knows their internal IT environment better than anyone, and everything is stored internally that helps in case of troubleshooting. It is more controllable and easily retrievable.	They are not more focused on industry threats and attacks. Mostly these type of intelligence is more concentrated on UBEA issues and common malware/virus threats. This intelligence may not give C-level executives an idea about evolving threats to organisations having the same business functions in the market. It does not cover digital brand protection that helps an organisation to understand how they are exposed on the Internet.
External (Outsourced)	It covers digital brand protection and also some unknown threats coming from the deep and dark web. It is more focused on evolving threats by correlating multiple intelligence sources across the globe, including paid, open-source and internally-developed. It reduces cost compared to internal intelligence infrastructure building. Organisations can leverage 24X7 support from vendors with best subject matter experts in various branches of security.	Vendors don't understand their client's infrastructure internally compared to internal company employees. Sometimes exposed data can be misused either by a vendor's internal employee or their third party.

Once you start collecting intelligence, it is must to make sure that it meets the organisation's requirement and business needs.

Data must be relevant to be used. A couple of questions can be considered in order to find whether that data is relevant to you or not:

- Does intelligence contain all types of data? (application level, network level and host level)
- Does intelligence contain data about all geography locations?
- Does it specific to your business type/function?
- How up-to-date is your intelligence data/feeds?
- Etc.

While we were in the planning phase, we determined the business need for threat intelligence. Once data is collected, that business needs must be aligned/mapped with the collected data before proceeding further.

Relying on free feeds can be harmful as it may not produce any actionable data.

If you are **outsourcing your intelligence**, the manager has to verify the reliability of collected intelligence by covering some key points as follows:

- data must be actionable
- data must be up-to-date
- data must be meeting their stakeholder's requirements
- quality of the data
- quantity of the data
- tailored/customised data
- third-party collecting data from trusted sources
- Does third-party verify data before presenting it to their customers
- Etc.

That's it for the third article. In the next article of Phase 3, I will talk about the analysis process and how it can be implemented more efficiently and effectively.