Integrate Threat Intelligence program into your daily security operations - Phase 1 - Planning and Preparation

From the last article located at **here**, we have now a majority of information to start the preparation and planning. In this article, I am going to explain how we can initiate the project and start preparing plans and procedures. This can be done in two phases.

Initial meetings with internal team to discuss the current threat landscape of an organisation.

Review observations that can help to prepare a perfect plan.

Initial meetings – In initial meetings with an internal team, we should discuss about current security measures in place and how they are being leveraged in order to be prepared against threat/attack. Discuss about existing tools, capabilities, human resources, procedures, escalation processes and plans. The outcome of this activity is to identify the current threat landscape and the existing security posture of an organisation.

To identify the current threat landscape, Threat intelligence team must understand the value of organisation assets. Following is the sample spreadsheet which can be prepared to present it to an internal team in order to find out all valuable organisation assets.

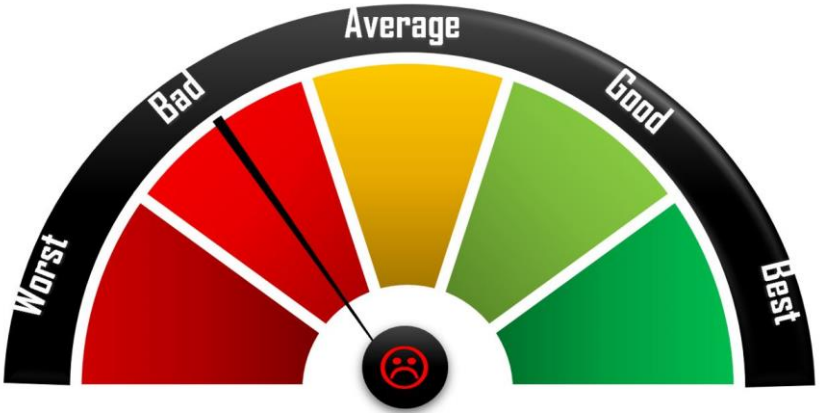
Table 1 - Risk Impact Coverage

Risk Areas	Description	How valuable this criterion is from risk perspective out of 100%.
Industry of business	XYZ organization's industry of business is e-Commerce, and they hold valuable data of their customers and vendors who sell items in it.	60%
Number of users	There are more than 5000000 users of our e-Commerce portal.	89%
Customer's data security requirement	Following customer data is stored within our database: – Name – Phone number – Address – Credit/Debit Card – Profile Pic – Purchase order history – Identity proof documents	58%
etc..	etc..	etc..
etc..	etc..	etc..

Likewise, there can be plenty of risk areas are there to be filled in this spreadsheet. An outcome of this activity is to derive charts which can show a potential risk area to specific valuable assets. Some of the sample charts are derived as follows where green, yellow and red are respectively Low, Medium and High:

Based on the above individual results, a summary of a risk to the whole organisation can be derived in the following chart:

All individuals and summary graphs can give an idea to a threat intelligence team that how much valuable data and information an organisation consume, which areas are more valuable from threat impact perspectives. This will help a team to prioritise their threat intelligence macro and minor activities.



Once we have the overall exposure analysis or an organisation, the next step involves the assessment of existing maturity of a threat intelligence capability. Threat intelligence project manager should create a set of questions to ask an internal team in order to identify the maturity of this activity. A team should have a baseline maturity level for each category and a data showcase and compare current maturity level with a target maturity level.

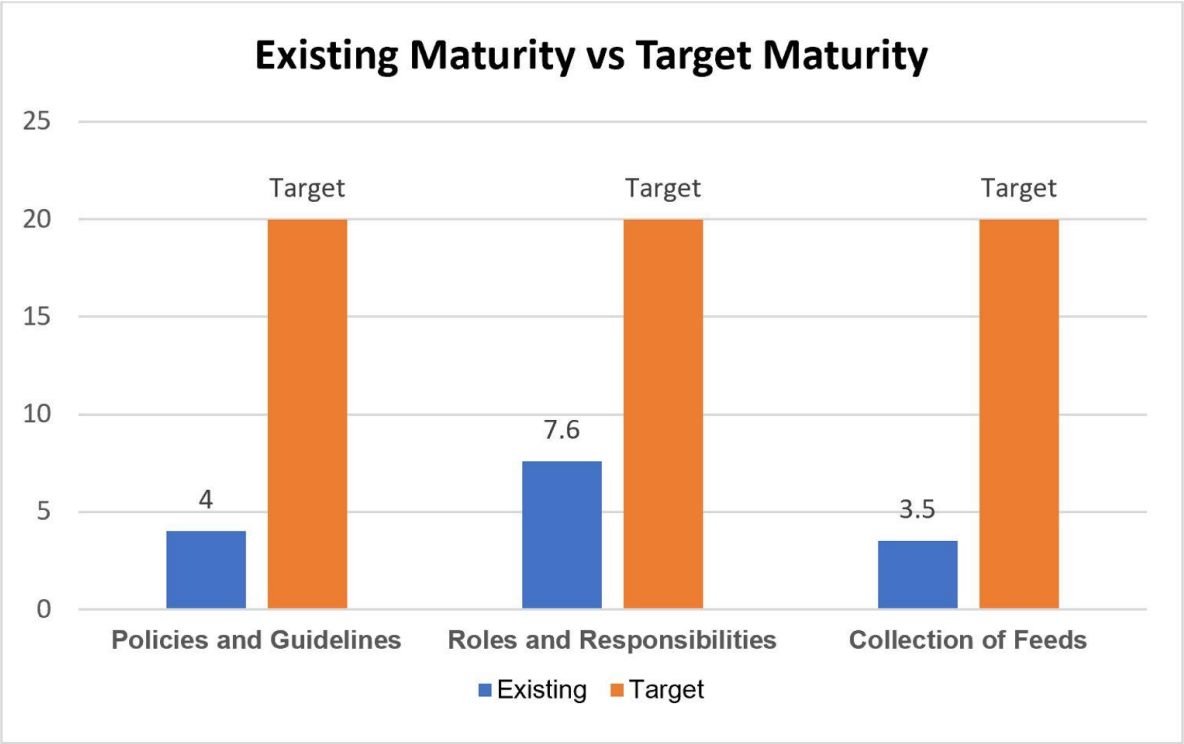
In this case, threat intel team's main objective is to identify whether an organisation has any threat intelligence maturity or not and if they have, how mature it is. Following is the sample spreadsheet of a questionnaire.

Table 2 - Maturity Analysis (Gap Analysis)

Category	Questions to ask	Results and Findings	Maturity Level out of 20
Policies and Guidelines	– Does an organisation have any Threat intelligence policies and guidelines? – How frequently are these documents updated? – Are those policies and guidelines being executed appropriately or not?	• The organisation does not have threat intelligence plans and policies document	4
Roles and Responsibilities	– Does your threat intelligence program have management roles and responsibilities? – Are your senior and junior resources sufficient enough to carry the entire program?	N/A	7.6
Collection of feeds	– How are intelligence feeds collected? – Which open source and commercial feeds are collected? – Are they integrated into your SIEM? – Is there a centralized feed management portal or dashboard? – Are feeds categorised based on categories to be actioned by different department of your organisation?	• Feeds are collected but not stored centralised • Feeds are not categorized in order to provide different teams within the organisation to act upon.	3.5
etc..	etc..	etc..	
etc..	etc..	etc..	

Review Observations

A sample chart to compare the current maturity of the program and target maturity can be presented as follows:



Based on the above gap analysis, the next step is to measure a cost of feeling gaps including necessary technical/non-technical resources and staffing. To feel the gap, the following areas must be taken into the considerations:

- Staffing (Human resources)
- Tools and technologies
- Managed activities within the operations
- Time required to complete all activities in one cycle
- Efforts required to complete all activities in one cycle

It is essential to influence the stockholders why this program is needed and what potential benefits an organisation can have from it. To influence stakeholders, a threat intel team should explain all challenges, problems, difficulties and risk areas of not having this capability such as:

1 – Impact of not having this capability –

Main risks involve:
• If breached, an organisation's reputation can be damaged
• Resignation of high-level executives
• Financial impact
• Lose of customer

2 – Value of having this capability –

Main benefits include:
• Threats can be blocked before it attacks your firm
• Improve overall security posture
• Productivity

To recap, as of now we have completed below activities:

- ✓ Initial kick-off meetings
- ✓ Identifying valuable assets
- ✓ Existing threat intelligence maturity posture and gap analysis
- ✓ Convincing stakeholders to implement this capability

Once all stakeholders agree to implement this capability, we need to document all planned activities to for the next phase (phase 2 – Design or implementation) in to reduce the current gap of a maturity posture.

It is crucial to protise all activities to execute it successfully. A sample spreadsheet prepared. The following chart is derived from the analysis performed in Table 1 – Risk impact coverage and Table 2 – Maturity analysis (Gap analysis):

Category	Activities to be completed	Priority	Hours required to complete activity	Initial Cost Required	Responsibility	Activity Completed	Status
Staffing and human resources	Hire 2 analyst and 1 manager for the entire activity	Optional (Should do)	7 <	$0	Chintan Gurjar	100%	Completed
Tools and technologies	Develop a centralised threat intel portal.	Mandatory (Must do)	15 <	$4000 - $8000	Ray Mateiro	100%	Completed
Managed activities	Develop a formal alert sharing template and plan	Optional (Should)	On-going	$0	John Cena	34%	Pending
Plans and policies	Document threat intelligence plans and procedure documents	Mandatory (Must do)	3 >	$0	Roy Miller	50%	Pending
	Develop an escalation policy.	Optional (Should do)	2 >	$0	Chintan Gurjar	70%	Completed
etc..	etc..	etc..	etc..	etc..	etc..	etc..	etc..
etc..	etc..	etc..	etc..	etc..	etc..	etc..	etc..

What to do next –

Now a threat intelligence team have a clear idea about how many technical and human resources would be required, what to prioritise first and last, how much time taking activities are these, etc.

As we have the necessary information to start the implementation, our last task before Phase 2 – Design and Implementation is to define a rough timeline for executing each activity. I am summarising everything with an ideal roadmap with a timeline to implement and perform all functions. This timeline may vary depending upon the organisation structure and size of the organisation. In the following timeline, I am covering the entire threat intelligence program by covering all macro and mini activities for one cycle:

0 to 3 Months (Preparation and Plan)
– Create all policies and plan documents
– Create roles and responsibilities
– Create escalation metrics
– Create RACI metrics
– Create formal processes, procedures and guidelines
– Create a formal reporting template
– Create a formal triage template
– Create a BCP and DR plan
– Create an incident response plan, procedure and guidelines

3 to 6 Months (Deployment and Data Collection)
– Deploy threat intel portal using SIEM
– Ingest feeds into SIEM
– Hire analysts with various skill sets
– Set up other necessary tools such as Splunk, etc.
– Design roadmap, goals and objectives.

6 to 10 Months (Data Collection)
– Collect feeds from various commercial and open source sources
– Setup continuous monitoring
– Deploy sandbox capability

10 to 13 Months (Data Analysis and Reporting)
– Analyze new feeds
– Eliminate non-required feeds
– Draft monthly, weekly report
– Draft yearly program maturity scoring result
– Draft overall security posture analysis every six months
– Publish threat advisory reports to clients and stack holders

Extra Mile
Here is some additional information to perform all activities with efficiency.

Feeds - While executing all these steps, make sure you collect all feeds from trusted and reliable sources, raw data does not make sense always. Raw data must be interpreted in a meaningful data to act on it. While you add all feeds in your threat intelligence platform or SIEM, make sure you are able to export all feeds in standard formats for future restoration in a different tool that supports standard feeds format.

What a plan document should cover - Create a threat intelligence plan document, and that should include Introduction, Glossary, Summary, Roles, Responsibilities, Plan, measures deliverables and success criteria's. As we are going to use a lot of short forms, the glossary section is needed to let everyone know the full form and meaning of those terminologies.

Essential role of threat analysts – We mentioned threat analysis term quite often throughout the article. While we are preparing plans and procedures, it is vital for us to define the most critical job functions of this entire program. Threat analysts play a vital role in this activity as they are the main show runners. Your threat intelligence platform must align with the MITRE framework to analysis of a threat and drafting a threat advisory report. A typical day of an analyst's life should include:

- Collecting IOCs from various trusted feeds either via automated or manual method.
- Categorizing and distributing IOCs within the team as per the skills requirement.
- Research about the latest APTs and threat actors active on the planet.
- Malware analysis and behavioural impact on a system and to an organisation.
- Preparing executive and detailed technical reports.
- Proactively hunting internal organisation assets to identify any unknown threats.
- Providing support for incident response.

To complete above all activities, various types of skilled resources are required. I have listed down primary skilled resources that an organisation may need in order to implement the threat intelligence capability:

Malware analyst – Who can reverse the malware, understand malware behaviour, impact on a system, identify the source of malware, understand signatures, sandbox analysis, identify indicators, etc.

Incident Respond consultant – Who is well-versed with the incident response process, runbook and guidelines, who knows how and what to act in case of crisis. A bridge between the technical team and executive level management team.

Penetration tester – Who can identify vulnerabilities, possible fixes, who can generate PoCs for newly or discovered vulnerabilities in the wild, who can educate the intelligence team to build a signature for new vulnerabilities and pretesting scenarios.

Depending upon how big and mature your threat intelligence model is, these requirements may vary from organisation to organisation. However, these are the basic mandatory requirement to start a service line. If we have the list or we know what kind of skilled resources would be required, we can create a list of skill sets to hire those people.

This is the end of the plan and preparation phase. In my next article, I will discuss how to design and implement the entire capability.