Integrate the Threat Intelligence program into your daily security operations - Phase 0 - Introduction

There is a huge amount of the increasing use of sophisticated malware, and often organisations fail to understand the real intent of such activities by a large group of hackers, nation-sponsored attacks, organized cybercrimes, cyber terrorists. These attacks result in revenue disruption, damaging public and private reputation and demolishing business processes and workflow.

Intelligence is staying ahead of the next threat targeting to your organisation by implementing protective measures to protect your brand reputation, data, people, process and technology infrastructure. I am assuming whoever reading this article has a little bit of background knowledge on threat intelligence terminology.

Just having a Threat intelligence product itself is not sufficient, data should be collected, classified and correlated with hacking tools, tactics and techniques.

Problems and Difficulties

Threat intelligence implementation cannot be possible without intelligence feeds. Open source free feeds are not sufficient enough to proactively detect all threats against your organisation unless and if you have a dedicated research team who is collecting all threat feeds from the surface web, deep web and darkweb. Intelligence feeds can often come in a variety of formats and sometimes may result in information overload. Such formats are malware feeds; intelligence feeds, social media intelligence feeds, people talking about your company in darkweb, company document leakage on darkweb and deep web, software threats and vulnerabilities intelligence feeds, nation-sponsored attacks intelligence feeds, etc.

Remember, information alone is not actionable. Intelligence provides so much data, but a company should align intelligence feeds with proactive measures' objectives to ensure the security to an organisation. If you are a third-party vendor and targeted, you can be the primary target of attackers to reach their final destination (which could be one of your largest customers as well).

Threat intelligence - 101

Typically when a company is breached, their C level executives (CISO, CTO, etc.) have these questions in the boardroom meetings and they want quick answers to these questions:

- **Who** are attackers?
- **What** are they attacking?
- **What** are their objectives/motives?
- **How** should we secure ourselves now and in future?
- **How** to identify these attacks?
- **What** are they using as a part of the hacking technique and tactic?

Threat intelligence, answers these questions. Threat intelligence is a risk management strategy to identify, detect, analyse and respond attacks before or while they are occurring.

There is a massive difference in threat actors of an early age and today's modern world. Previously organisations were mostly facing threats from cyber criminals and former employees who were acting either alone or in a small number of groups where these days there is a range of new threats coming from nation-state hackers to carry cyber espionage, sabotage and warfare to other countries, militaries, foreign governments. Hacktivist groups such as Anonymous, LulzSec, Lizard Squad, Syrian Electronic Army etc. Terrorists using a cyber world to spread fear and terror using social networking websites. Competitors hire third-party hackers for digital espionage.

Threat intelligence is all about collecting and analysing IOCs (Indicator of Compromise). There are two types of indicators:

Behavioural – If a chain of hacking tactics, techniques and tools are used to compromise a target, it falls under behavioural IOCs. For example, hackers use spear phishing technique to plant malware on their target system.

Data Derived – These types of IOCs are usually straightaway identified from the information involved in the incident such as malware name, malware hash value, domain name, etc. In this case, normally analyst takes one piece of information and searches it on the Internet and within the intelligence feeds. If the same sample is found acting in another part of the world, they can find or request technical analysis of that particular IOC.

Tactics, Tools and Procedures (TTP) – If an organisation can identify TTP quickly, it will help them to plan a response in a quick time. TTP can involve actor tactics, hash values, IP address, domain names, URL, email address, etc.

Cyber Kill Chain – It's a process used by attackers. The blue team must align itself with the attacker's cyber kill chain to proactively mitigate threats.

Threat intelligence cannot be served as a standalone program. It must collaborate with vulnerability management and security operations. Most of the companies are operating a variety of tasks independently such as threat analysis, network monitoring, end-point security, incident response, etc. If these processed are joined along with threat intelligence service, it can add more value to an organisation. For that following best practices are required to be followed:

- Establish an accessible channel of communication between all security departments
- Set up roles and responsibilities with escalation metrics.
- Develop a central feed portal to integrate all service's result
- Executed well-established processes and procedures followed by comprehensive monitoring

A successful threat intelligence program should include:

– Collecting IOCs and IOAs. Indicators of attack and Indicators of compromise
– Identify threat actors such as
  o IP address
  o Domain watchlist
  o URL watchlist
  o C2 (Command and Control)
  o Group name or organisation name of hacktivists
  o Malicious email
  o File names and hashes
  o Intend of attacks
  o Malware samples
  o Network traffic communication
– Processes and procedures to understand and identify attack methods such as:
  o Spear phishing
  o Macro execution
  o Drive-by-compromise
  o USB dead drops
  o Payload execution

Every attack method is covered in the MITRE framework

– Data analysis methods to analyse feeds or potential IOAs or IOCs.
– Incident management and response processes to improve response and recovery time.
– Escalation and reporting procedures and processes.

Benefits of building a Threat Intelligence Platform

– Internal defences get stronger and effective
– Detecting before a breach happens saves a lot of cost of a company and it also protects your brand reputation
– Finding unknowns attacks and tactics before it impacts your organisation
– Provides third party protection
– Optimises internal processes
– Identification of attacks not detected by traditional NGAV and other security defences
– Provides excellent visibility into the threat landscape
– Provides greater visibility into insider threat
– Identify threat in the earlier cyber kill chain
– Prioritise threat indicators of potential events
– It has a lot of strategic and operational level benefits too.

How many resources it may require to implement the entire program and use it for the first time.

Here I am assuming that this entire statistics and planning is applicable for SMEs and small firms having employees between 200-400.

Phases	Objectives	Resources Required
Phase 1 – Preparation	– Performing shadow IT activity to analyse the entire scope of an organisation from a threat perspective – Identify what security measures are in place and how organisations dealing with the current threat and space – Distinguishing all high priority targets – Developing a team – Developing plans, processes and procedures	**Time and resources required for this activity:** 1 Senior Intelligence Executive – 3 days 1 Intelligence analyst – 3 days 1 Project manager – 3 days
Phase 2 - Deployment	– Deploying a vendor-based solution – Configuring solution according to client's need – Deploying open source TI tools and techniques along with a professional solution – Integrating it to the SIEM – Creating BCP and DR plan for the entire platform	**Time and resources required for this activity:** 1 Senior Intelligence Executive – 2 days 1 Intelligence analyst – 5 days 1 Project manager – 2 days
Phase 3 – Data Collection	– Collect all sort of feeds/data – Categorise them department wise and feed	**Time and resources required for this activity:** 1 Senior Intelligence Executive – 1 day 1 Intelligence analyst – 1 day
Phase 4 – Data Analysis	– Identify data/feeds – Perform analysis on data/feeds – Understand the analysis criteria/roles and responsibilities – Optimize a large amount of data/feeds to align with your objectives for proactive hunting	**Time and resources required for this activity:** 1 Senior Intelligence Executive – 3 days 1 Intelligence analyst – 7 days 1 Project manager – 3 days
Phase 5 – Reporting	– Produce actionable intelligence alerts and briefings – Produce a weekly/monthly/daily report	**Time and resources required for this activity:** 1 Senior Intelligence Executive – 1 day 1 Intelligence analyst – 4 days 1 Project manager – 1 day

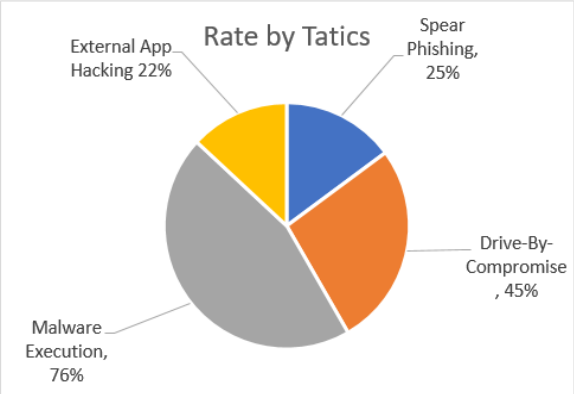
Keep a track record of Statistics monthly/weekly/Yearly

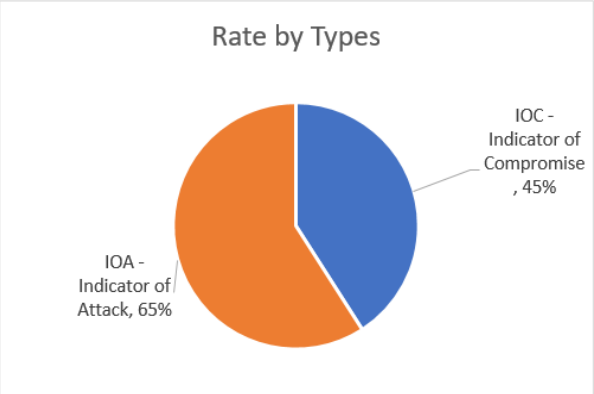
Following areas must be calculated statistically on a regular period to define the overall state of the security over the period before and after the threat intelligence process is implemented:

– Number of incidents
– Number of IOAs
– Number of IOCs
– The false positive/negative rate

– The true positive/negative rate
– Response time rate
– Internal and external threat
– Threat type rate
– Attack techniques/tactics rate

Following are the two examples of statistics tracking on a monthly, weekly basis:





Reference

http://www.waverleylabs.com/will-the-software-defined-perimeter-debunk-the-cyber-kill-chain/s