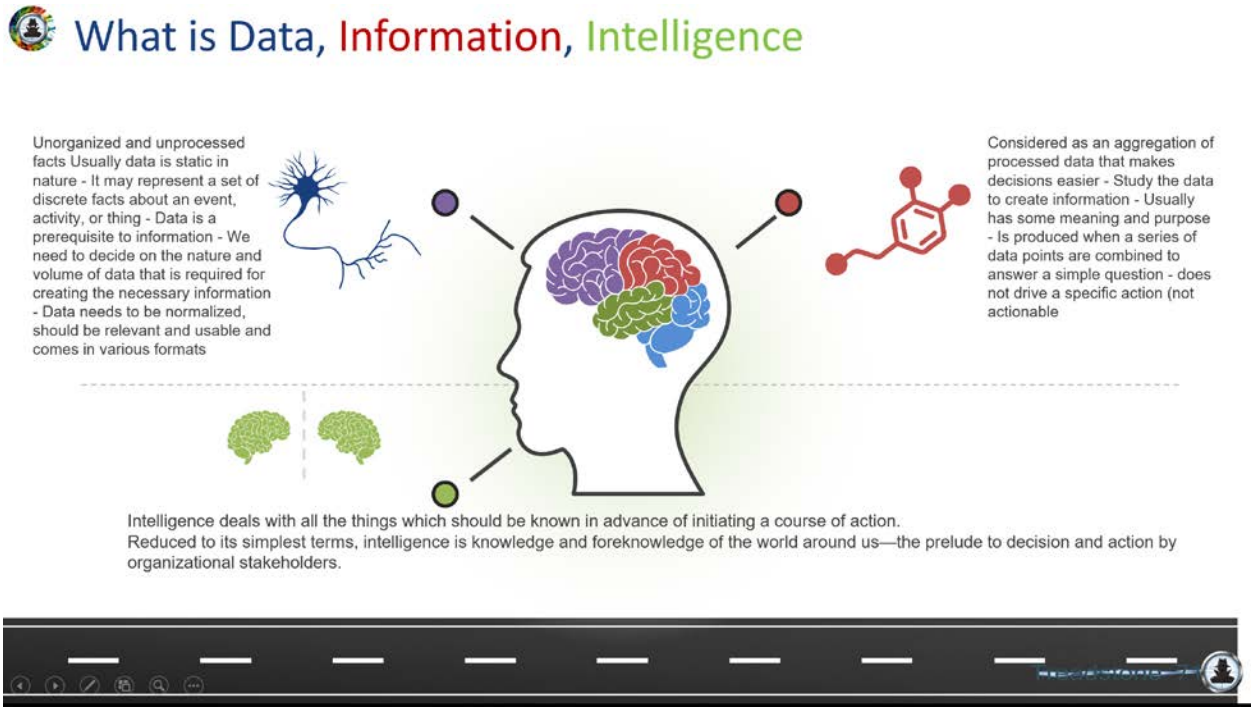
Stakeholder Brief - Understanding Intelligence

Organizations follow inaccurate definitions of threat intelligence leading to poorly conceived cyber threat intelligence programs. Vendors communicate threat intelligence definitions supporting their offerings propagating the fallacy that threat intelligence solves numerous security problems.

Cyber Threat Intelligence functions being built on a foundation that are not supported by standard intelligence tradecraft. Many programs support a fraction of the intelligence needs yet stakeholders hold unrealistic expectations based upon expenditures.

Information security capabilities marginally improve as spending skyrockets and security posture improvement is limited to after-the-fact discoveries communicated as prevention. Hunt and detect is not prevention when the hunting occurs inside your perimeter.

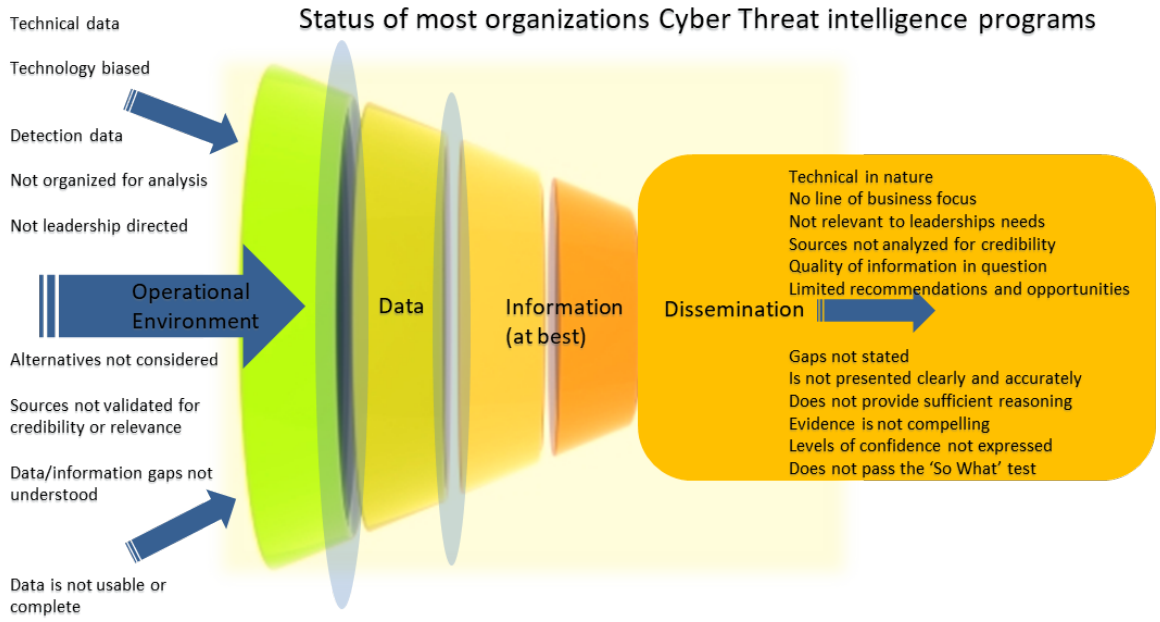
Continued purchases of 'threat intelligence' tools based upon the see-detect-and arrest paradigm ensures slow improvement and 'loss of data' expansion. Intelligence program builds focused on technology capabilities repeats the historical problems of information security when firewalls and anti-virus represented the core of security programs. You do not build an army around an M-16. You use the M-16 as a tool to attack and defend.



Treadstone 71 – Taken from Fallacies and Faultlines - https://cybershafarat.com/2017/06/27/fallacies-and-faultlines-cyber-threat-2/

A general Internet search on 'threat intelligence' returns 11 million results in .36 seconds demonstrating the intentional propagation of a term intended to generate revenue. Information and cyber security vendors, well-known training organizations, and companies use the term so often it has lost any real meaning. Most vendors use the term as if intelligence is easily created and available like fruit from a tree. Products are sold with the expectation that threat intelligence is the panacea CISOs have sought for years. This is a general misnomer and cyclical in the regular creation and use of buzzwords and catch phrases that change annually. Vendors create years of capabilities based upon the jargon that just yesterday, no one even knew existed. One of those buzzwords is threat intelligence. Therefore, we have spent time defining data, information, and intelligence.

Threat intelligence is a subset of intelligence. Threat intelligence assumes a certain amount of data and information is collected creating intelligence that is then aligned to organizational threats. Threat intelligence does not always include the correct data. Most all times, the data is tactical and technical in nature leaving significant gaps. Other times that data is skewed by the inherent bias of the technologies through which it is collected and filtered. In the end, it lacks in scope, depth, breadth, and is deficient with respect to tradecraft. Other types of intelligence reporting rarely covered in organizations include, basic and foundational intelligence, research intelligence, competitive, and estimative intelligence. Traditional warning intelligence is what the information security industry calls threat intelligence.



What is Tradecraft?

Unfortunately, most of what is produced are data and at best, information. This starts with the misunderstanding as to what data is versus information as opposed to actual intelligence. The term is a core component of sales neglecting the difficult process of creating intelligence, while presenting data

and information as actionable intelligence. Creating intelligence is a process that requires hard-nosed collection, attention to detail in production, structured methods and techniques, awareness of critical thinking and cognitive bias, the use of analytic methods, and the patience and perseverance that comes with knowledge creation. This is called tradecraft. Indicators of compromise are items of data. The name and location of an adversary are items of data.

Let us not confuse tradecraft as being military intelligence. Many believe intelligence tradecraft is military in form and function. This is not true. The intelligence tradecraft of which I speak is rooted in intelligence community capabilities honed over years of trial, error, mistakes, and triumphs. The use of intelligence tradecraft enables organizations to see beyond the limited view of 'see, detect, and arrest' while progressing to data collection, analysis, and intelligence creation used to prevent and eventually predict adversary actions. In addition, tradecraft is the underlying framework for intelligence upon which military and non-military programs should be built.

Many of the fallacies we face as cyber security professionals relate to a lack of understanding of what it takes to be an intelligence professional. The two are not mutually inclusive. Security operation centers are not populated with intelligence professionals. They are not occupied by analysts skilled in intelligence. In fact, most cybersecurity professionals find tradecraft to be distasteful and a general waste of time. This conclusion is drawn from the many engagements across the globe with cybersecurity professionals. When we come onsite to help build the intelligence program, we immediately face resistance if the focus is not on low level, technical activities. Yet most do not have a grasp, respectfully, surrounding the need for a well-built intelligence program that is top-down as opposed to technically oriented, bottom-up. Most have not had training in intelligence analysis or tradecraft. Real world intelligence analysts endure rigor, structure, focused training that specializes in the craft of intelligence analysis. The core function of any intelligence organization. They learn how to think, write, and brief. They study analytic tools, counterintelligence issues, denial and deception, analysis, and warning skills.

Another fallacy is that former military intelligence soldiers and National Security Agency staff are skilled in tradecraft. Not to say that they are not capable or that they have not had intelligence courses but the courses are focused on physical, military action. Their version of tradecraft is specific to their missions and requirements. The NSA trains collectors to collect and analysts to analyze and most times, never the twain shall meet. We have direct knowledge of these methods. The protocol is compartmentalization and separation of duties as a higher priority over continuity of effort and understanding. The intent here is to point out that their skills are very focused on many different areas associated with intelligence. Whether the type is signals based or human, the methods do not include the end-to-end scope of traditional intelligence tradecraft. What we have found is their adoption to be much faster, their understanding of the model more inclusive than cyber security professionals. In general, the ability to adapt, adopt, and incorporate the tradecraft model is not a stretch for these men and women due to their backgrounds.

The Daily Crises

We spend countless hours preparing daily reports, responding to daily incidents, and dealing with the issue de jour. Morning stand-up meetings are preceded by a daily data push many call intelligence. It is not intelligence in most cases but daily news. We establish serialized reporting where each day we deliver a threat report; each week a weekly threat rollup; each month a rollup of each week and so on. We spend so much time gathering current data and fighting daily issues we never get to a point where we can perform intelligence-type work This is largely self-inflicted. This fallacy in our process ensures we will never have the ability to analyse data based upon historical collection. The collected data is all current. The scope for that data is immediate. The data is not arranged in such a way as to facilitate long-term analysis. Of course, there needs to be a balance between the long-term analysis and the short-term reporting. The fallacy is that the short-term reporting is communicated as intelligence analysis product when it is mostly a regurgitation of open source data and readily available vendor reports.

Fallacies that Create Fault Lines

As discussed above, we believe the fallacies in intelligence stem from a lack of agreed upon glossary and taxonomy and, an overall understanding of what it is. This is because most approach intelligence from a tool perspective as driven by vendors selling product. In addition, the industries acceptance of vendor solutions to provide actual intelligence, and vendor reports taken at face value without source validation or citation. The organizational placement of intelligence within information security, many times incident response as well as the inaccurate understanding of what an intelligence professional is, and the inability of organizations to see beyond purely defensive measures for information security all contribute to the issue. These fallacies, understood to be non-inclusive, create inherent fault lines in our security programs.

Recommendations and Opportunities

Changing Behaviours

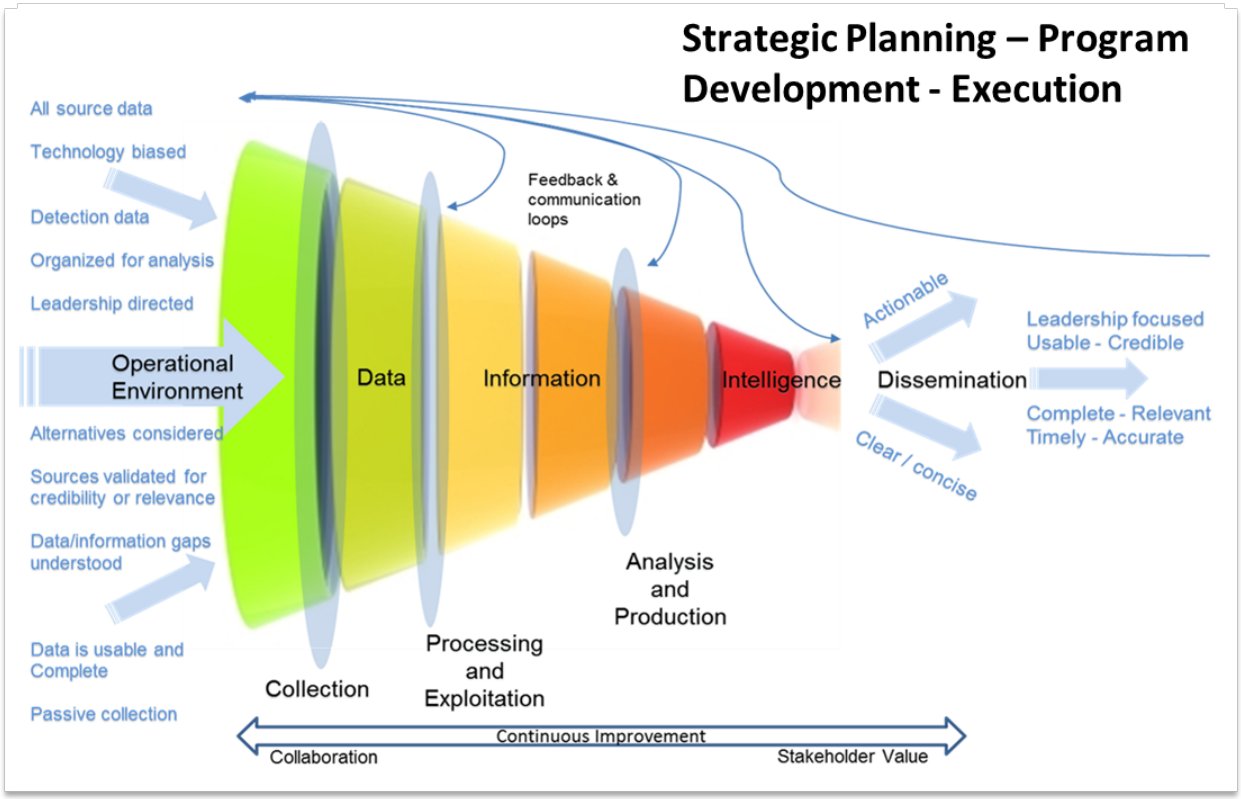
What can we do to rectify the path of fallacies we continually choose to follow?

First (in no specific prioritized order) we must educate everyone in information technology, information security, and the C-Suite on the standard taxonomy of intelligence. This provides a shared understanding and baseline glossary upon which to build communication.

Secondly, we must treat each vendor report as nothing more than another source of data. Data that must be evaluated for credibility, reliability, and relevance. To do so, we can use the NATO Admiralty Code to help organizations evaluate sources of data and the credibility of the information provided by that source. Evaluate each vendor report using this coding method while documenting ease of data extraction, relevance to your organizational issues, type of intelligence (strategic, operational, tactical, and technical), and value in solving your security problems. Several TIPs have started this process but they do not have the underlying methods of scoring to back up their selection of the A to F and the 1 to 6.

Treadstone 71 – Taken from Fallacies and Faultlines - https://cybershafarat.com/2017/06/27/fallacies-and-faultlines-cyber-threat-2/

Thirdly, begin to grow and expand your intelligence program functions. Learning methods of anonymity, open source data collection, collection management and planning, production management of intelligence functions, analysis, and analytic writing and dissemination adds immediate value to your organization. Understand that intelligence is not the same as incident response or a core component of the security operations center. These skills are unique and must be shared but to bury them within these areas is a mistake. We faced this for years (and still do) putting information security under information technology treating it as a solely technical issue. We should not make the same mistake with intelligence. Intelligence functions need direct access to organizational stakeholders.



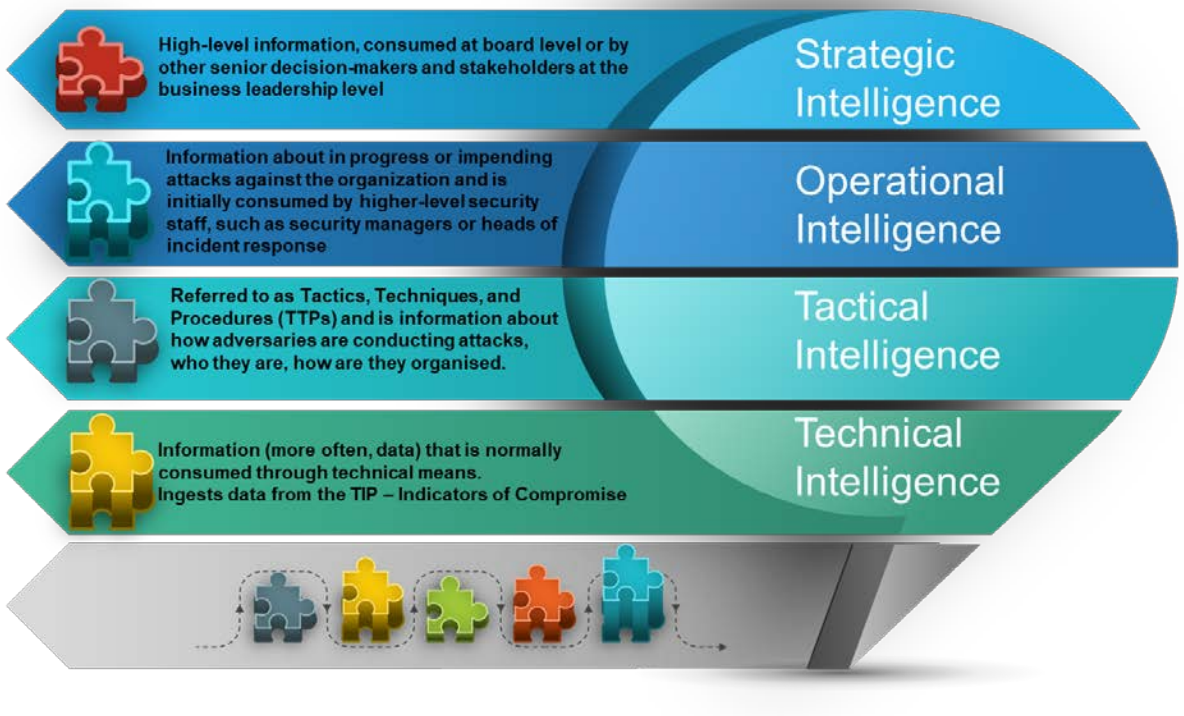
Fourth, create standard processes to seek out malicious actions within your information technology environment. Use adversary TTPs to drive your 'hunt and detect' but understand that albeit a valuable capability, is not a proactive function. They are already inside the wire and must be removed. Organizations need to do this for proper hygiene.

Fifth, develop methods within your organizational risk model to collect open source data regularly. Like our third point above, we must grow this function so we collection data and information, and develop intelligence that is pertinent to our stakeholders and our organization. Capture priority intelligence requirements, create information requirements prioritized and vetted focusing on all sources of data

including open source collection. Devise methods for mission management that drives targeting for passive collection.

> Make note that many vendor report subscriptions provide generalized and generic data and information. Periodically, intelligence is part of the report. Occasionally, something relevant to your organization is included. Most time the reports are of a create once, distribute many format that needs localisation.
>
> To drive industry change, work with vendors. Request and require source credibility ratings, citations with confidence levels, explanations of analytic methods, and resumes of staff working your contracts.
>
> To drive industry change, we must become the model that all seek to emulate.

Sixth, create a model of your adversaries and their capabilities that are target centric. Expand your



collection to include all areas concerning your adversary. The only way to fully understand what threatens your organization is to fully understand the enemy, their motivations, their competence, and their skills. Otherwise, organizations will continue to play a basketball game on defence, never crossing the half-court line. A recipe for assured loss.

Treadstone 71 – Taken from Fallacies and Faultlines - https://cybershafarat.com/2017/06/27/fallacies-and-faultlines-cyber-threat-2/

Seventh, write in intelligence analysis format. Stakeholders have little time. Making them hunt for the answers ensures failure. Use the guides provided to assist in your writing, Intelligence Analysis Format.
Eighth, create a strategic plan followed by a program plan for intelligence in your organization. Define what it is and is not. Author a vision and mission along with guiding principles. Develop a series of goals with three to four objectives each determining how to achieve those goals. Gain acceptance and follow the plans.

Ninth, set up a listening tour of your lines of business and corporate stakeholders (Stakeholder Analysis). Gain permission to attend their meetings with the understanding that you are there to listen and learn. Do not offer your services. Listen to digest and gain knowledge of your stakeholders. Do not listen to prepare a response. Gather this information and take it back to your organization to help your program move forward. You may believe you know your company but knowing your professor ensures an 'A.'

Tenth, give your organization time to implement an intelligence function. Determine what makes sense for your organization as to what that timeframe is. Institutionalize lesson-learning as process of performance improvement, not assessing blame. Give your intelligence organization time to learn. Making mistakes in the preliminary stages of maturity is expected. Just do not make the same mistakes repeatedly. Give your intelligence organization the authority to make decisions and the access to stakeholders to learn requirements and communicate capabilities. Establish goals and objectives that are reachable and practical. Stretch goals when first building a function can lead to unnecessary failures. Leadership and the right level of leadership is required to manage analysts. Find the right level for your organization. When you add an intelligence function to an organization that has never had one, manage expectations. Eventually, a properly staffed, trained, and led group can delivery significant value to the organization.

Lastly, although non-inclusively, prepare your organization for the next steps. Use the soon-to-be-released Treadstone 71 Cyber Intelligence Maturity Model. Those next steps involve counterintelligence. Although now seen as a high-risk area for organizations, my belief is that we will eventually adopt certain principles associated with this tradecraft. In fact, several organizations already employ methods associated with counterintelligence, both passive and active

Cyber Intelligence Maturity Model - ®Treadstone 71	6 Months	12 Months	18 Months	24 Months	30 Months	36 Months
Introduction to Intelligence	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Stakeholder Management	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Collection Management	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Collection	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Requirements Management	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Mission Management	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Situational Awareness	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Critical Thinking	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Creative Thinking	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Cognitive Bias	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Structured Analytic Techniques	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Production	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Analysis and Analytic Issues	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Analytic Writing	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Reports and Dissemination - Analytic Briefing	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Integration	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Administration - Standard Operating Procedures	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Evidence	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Argument Mapping	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Threat Intelligence Platform	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized
Sharing	1 - Initial	2 - Repeatable	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed
Case Studies	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	4 - Managed	5 - Optimized

Much like information security a short 15-20 years ago, cyber intelligence is in its infancy and misunderstood. We are rife with fallacies, inaccurate definitions, and terminology usage. The profession of intelligence should not be confused with security and should not be clouded by poor and biased reporting. The only way to change the problems inherent in intelligence today is to drive that change internally while forcing the market to shift. The intelligence community realized this years ago striving to create the 'profession of intelligence analysis.' The framework of intelligence can and should be the underlying standard for intelligence planning and program builds. Placing intelligence inside a defensive-focused organization tuned to triage and remediate ensures and effective see, detect, and arrest program. A program that will not keep malware and adversaries out of your environment.

Pros and Cons of putting intelligence inside the SOC organization

Pros –

- Addresses immediate concerns with TIP implementation and usage
- IoC tagging and tag management
- Rapid review of IoCs for hunt and detect
- False positive review and clean up

Treadstone 71 – Taken from Fallacies and Faultlines - https://cybershafarat.com/2017/06/27/fallacies-and-faultlines-cyber-threat-2/

- Vendor report review for credibility, reliability, and potential overlap
- Tied directly to incident response for triage and remediation
- Identify changes in IoC capabilities and targeting
- Build adversary dossiers and TTPs
- Works directly with those in charge of malware reverse engineering/forensics for technical analysis
- Create technical reports
- Valid TIP technical processes and procedures

Cons –

- Purely technical view without business awareness
- Limited interaction with other security staff
- The TIP will only be used to IoCs with some TTP activity
- Limited knowledge of adversary campaigns – a heads down approach to technical/tactical intelligence
- Limited knowledge of overall organizational attack surface and situational awareness
- Limited reporting for the business and organizational leadership
    - Reporting is of a technical nature and not aligned to business concerns
- Intelligence capabilities do not grow with industry demands and needs
- Limited job growth potential
- Analysis is not matured only focusing on technical issues
- No time for analysis due to incidents
- Analysis is not strategic
- Limited to no OSINT collection of target information and adversaries to your organization
    - (vendor info is financial services generic)
- No alignment with business intelligence and competitive intelligence
- Limited to no awareness of an organization's new products and services (after the fact)
- All activity is after the face (see, detect, arrest) – not proactive or preventative
    - IoCs detected already in your organizations environment
- TIP usage limited to technical and operational issues
    - % usage of TIP functionality low
        - Ignores other features and functionality that are not SOC focused
- Limited sharing at a business level
    - Sharing consists of technical and tactical data that is based upon after-the-fact discovery
    - The model is based upon a failed model steeped in police methods of see, detect, and arrest that is proven to fail (years of breaches and data loss)
    - The Lockheed Martin kill chain is based upon see, detect, and arrest
    - The Mitre ATT&CK model is based upon after-the-fact information
        - Both are needed but are components of the failed model

Intelligence includes the need for see, detect, and arrest but best serves and organization when used to predict and prevent.

The Intelligence functions should stretch throughout the organization and is embedded within all areas, while being led from the top down based upon tradecraft tied to the business. Do not build your program based upon a tool.

JSB