ESTABLISHING CYBER THREAT INTELLIGENCE

MUNEEB IMRAN SHAIKH

CISSP CCSP CRISC PMI-ACP CDPSE COBIT 2019 Foundation

https://www.linkedin.com/in/muneebimranshaikh/

Table of Contents

WHAT IS CYBER THREAT INTELLIGENCE & WHY IS IT NEEDED 2
DATA VERSUS INTELLIGENCE 2
TYPES OF THREAT INTELLIGENCE 3
Strategic Intelligence 3
Operational Intelligence 3
Tactical Intelligence 4
INTELLIGENCE VERACITY 4
WHAT MAKES GOOD INTELLIGENCE 5
ESTABLISHING A CYBER THREAT INTELLIGENCE FUNCTION 6
1. VULNERABILITY MANAGEMENT 7
2. SOC/INCIDENT RESPONSE TEAM 8
2.1 MEASURING DEFENSE CAPABILITIES AGAINST ADVERSARIES 8
3. SECURITY LEADERSHIP & RISK MANAGEMENT 9
4. FRAUD MANAGEMENT 11
UNDERSTANDING CYBER UNDERGROUND MARKET 12
THREAT INTELLIGENCE PLATFORM INTEGRATIONS WITH OTHER SECURITY SOLUTIONS 14
CHALLENGES RELATED TO THREAT INTELLIGENCE INGESTION 15
RELATIONSHIP BETWEEN THREAT INTELLIGENCE AND THREAT HUNTING 16
CONCLUSION 18
APPENDIX: List of Acronyms 18
REFERENCES 19

WHAT IS CYBER THREAT INTELLIGENCE & WHY IS IT NEEDED

Humans have historically relied on Intelligence to make assessments, understand its implications and plan accordingly. Nations have relied extensively on Threat Intelligence in the military realm to plan their kinetic operations and establish their defenses to achieve their objectives and goals.

In the conventional warfare, you need to understand the capabilities, motivations and goals of your adversaries. In kinetic operations, groups at conflict, try to impair and destroy the capabilities of their adversaries first and later attempt to engage in subsequent battles within a war.

The damage to the capabilities becomes pivotal because it has psychological impact on a group's morale, capability to respond back or defend itself from any aggression. With the evolution in threat landscape over the years, the usage and application for threat intelligence has also evolved.

Cyber Threat Intelligence is the analysis of cyber threat actors, their capabilities, motivations, and their goals. Such analysis allows organizations to prevent and mitigate cyber-attacks on their organizational infrastructure and assets.

It is unfortunate that Cyber Threat Intelligence has become a buzzword for many to be used with their own interpretation and its implementation is often limited to the consumption of threat data feeds which are often volatile and tactical in nature and therefore do not add value to the *strategic objectives* of the Organization.

DATA VERSUS INTELLIGENCE

One of the common issue is the misconception around Intelligence & Data. Often these two terms are used interchangeably therefore it is essential to establish the distinction between the two terms.

Data is a piece of information, fractional fact that requires further analysis. Data is often represented in the form of Threat indicators such as IPs, Domain Names, Hashes etc. but they do not provide context behind threat actors, their motivations and objectives without thorough analysis.

Intelligence is contextualized actionable information derived through collection, processing and data analysis and is meant to provide context around data.

Scott J. Roberts & Rebekah Brown, in their book Intelligence Driven Incident Response highlight:

"The difference between data & true Intelligence is Analysis. Without analysis, most of the data generated by the security industry remains as data. That same data, however, once it has been properly analyzed in response to requirements, becomes intelligence, as it now contains the appropriate context needed to answer questions and support decision making."

TYPES OF THREAT INTELLIGENCE

Threat Intelligence is an actionable information that equips its consumers to make informed decisions therefore it is important to understand the distinctions among Threat Intelligence category and its audience. An Intelligence that does not reach the right audience is considered to be wasted therefore it needs to be curated and positioned appropriately for enabling its consumers to make informed decisions.

Intelligence varies in their sources, audiences, and the formats they are presented in.

Strategic Intelligence is meant to support C-Suite executives and board of directors in making informed decisions about their business strategy keeping in view the existing business drivers and trends around which they have to steer the organizational strategy, conduct Risk Assessments, and allocate resources accordingly.

In one of my earlier paper "*Cyber Threat Intelligence – A Partner in Risk Management*", I've explained how Cyber Threat Intelligence Function can aid Risk management function. Strategic Intelligence provided to Senior Executives helps them to understand the broader Cyber Threat Landscape, existing threat actors operating in your industry vertical or in the region, their motivations and the manner in which they've choreographed their previous attacks.

Developing Good strategic intelligence reports require sound and thorough analysis conducted by Threat Intelligence Experts on the observed adversarial tactics, techniques and procedures to subvert the Security Controls. It is essential that Strategic Intelligence Reports are written in a business oriented language which can be easily understood by the Senior Management.

Type of Intelligence	Type of Information	Format	Customer
Strategic Intelligence	High Level Information about Observed Attacks, Threat Actors & their Motivations	Reports, Briefings, Power Point Presentations	C-Level Executives. BoDs

Operational Intelligence is the bridge that helps to link the Strategic Intelligence with the Tactical Intelligence.

As mentioned above, Strategic Intelligence is about understanding the various threat actors' motivations and objectives, Operational intelligence is concentrated towards understanding the campaigns and high-order TTPs associated with threat actors.

Operational Intelligence helps to understand if the exploitations seen are targeted towards a specific victim or driven by opportunity and what kind of malwares or other tools are used by different threat actors in pursuit of their goals.

It is particularly important for incident responders, SOC Managers or Senior SOC Analysts to help them understand the broader Cyber Threat Landscape.

Type of Intelligence	Type of Information	Format	Customer
Operational Intelligence	- Campaigns Information. - Malware Intelligence - Vulnerability Exploitations/PoCs	Reports, Briefings, Scripts, Signatures,	Incident Response Team. SOC Managers Senior SOC Analysts DFIR

Tactical Intelligence is highly volatile information represented in the form of IoCs, Observables or Threat data feeds containing discrete information about the attacks.

Examples include Command & Control Server IPs, Hash Values for the Malwares deployed as the tool to perform exploitations & infrastructure used to perform scans for vulnerability searching.

Tactical intelligence is discrete and technical in nature and therefore helps the Security Operations or Incident Response teams to detect and understand context of anomalies observed and establish defense mechanisms accordingly.

Type of Intelligence	Type of Information	Format	Customer
Tactical Intelligence	- IoCs. - Observables	- Reports, - Text Files - Scripts - Signatures	Incident Response Team. SOC Teams CTI Analysts

INTELLIGENCE VERACITY

While consuming the Threat Intelligence (Strategic, Operational or Tactical) we must remember the main objective of having an effective Threat Intelligence function is to help organizations make informed strategic decisions, understand broader Cyber Threat Landscape and establish defense mechanisms to guard against any Compromise, therefore understanding the veracity or confidence level tied to each intelligence is important.

These Confidence Levels reflect the accuracy and correctness of information contained in Threat Intelligence, based on the level of trust from Threat analyst who has worked on the intelligence.

The Confidence Levels are reflected as *Admiralty Code* and are combined of "*Reliability of Source*" & "*Degree of Confidence*" and range from A1 – E5.

Admiralty Codes	
Reliability of Source	**Degree of Confidence**
A (Reliable) – E (Unreliable)	1 (Confirmed) – 5 (Improbable)

EXAMPLES	
A1	Reflects that Information came from the Reliable source with a history of information
E5	Reflects that Information came from an Unreliable source and it is improbable for the information contained to be True.

WHAT MAKES GOOD INTELLIGENCE

Scott J. Roberts & Rebekah Brown, in their book Intelligence Driven Incident Response highlight the Characteristics of Quality intelligence which relies on:

1. *Collection sources*
2. *Analysis*.

Collection Sources & Context:

It is fair to say that investigate journalism and Threat Intelligence have certain common principles, just as a good journalist is considered not to burn his/her sources. Likewise the Threat Intelligence providers may not always provide the source of their intelligence. However the Intelligence is primarily generated and collected either through Incident Investigations, Forensic Analysis or via Honeypots.

An understanding of Intelligence whether sourced through investigations or machine driven (honeypots, Network Sensors, Tarpits etc.) provides valuable contextual information for better analysis and action.

Additionally the Date of Intelligence Collection is equally important because the majority of cyber-threat data in the form of IoCs is perishable and may not be relevant all the time. Understanding when data was collected can help defenders understand how it can be acted upon.

It is therefore important that you have functional policies in your Threat Intelligence Platform to retire or expire the low level perishable threat data to avoid stocking of Indicators which may not add value.

Context also includes other additional details that help to construct the entire jigsaw puzzle.

Addressing Biases in Analysis

Humans have varying perceptions of similar ideas, observations or facts which lead us to pivot in a certain direction and cultivate conscious or unconscious biases. It is natural for a Threat Analysts to have biases however countering those biases is imperative and will be discussed in following section with further detail.

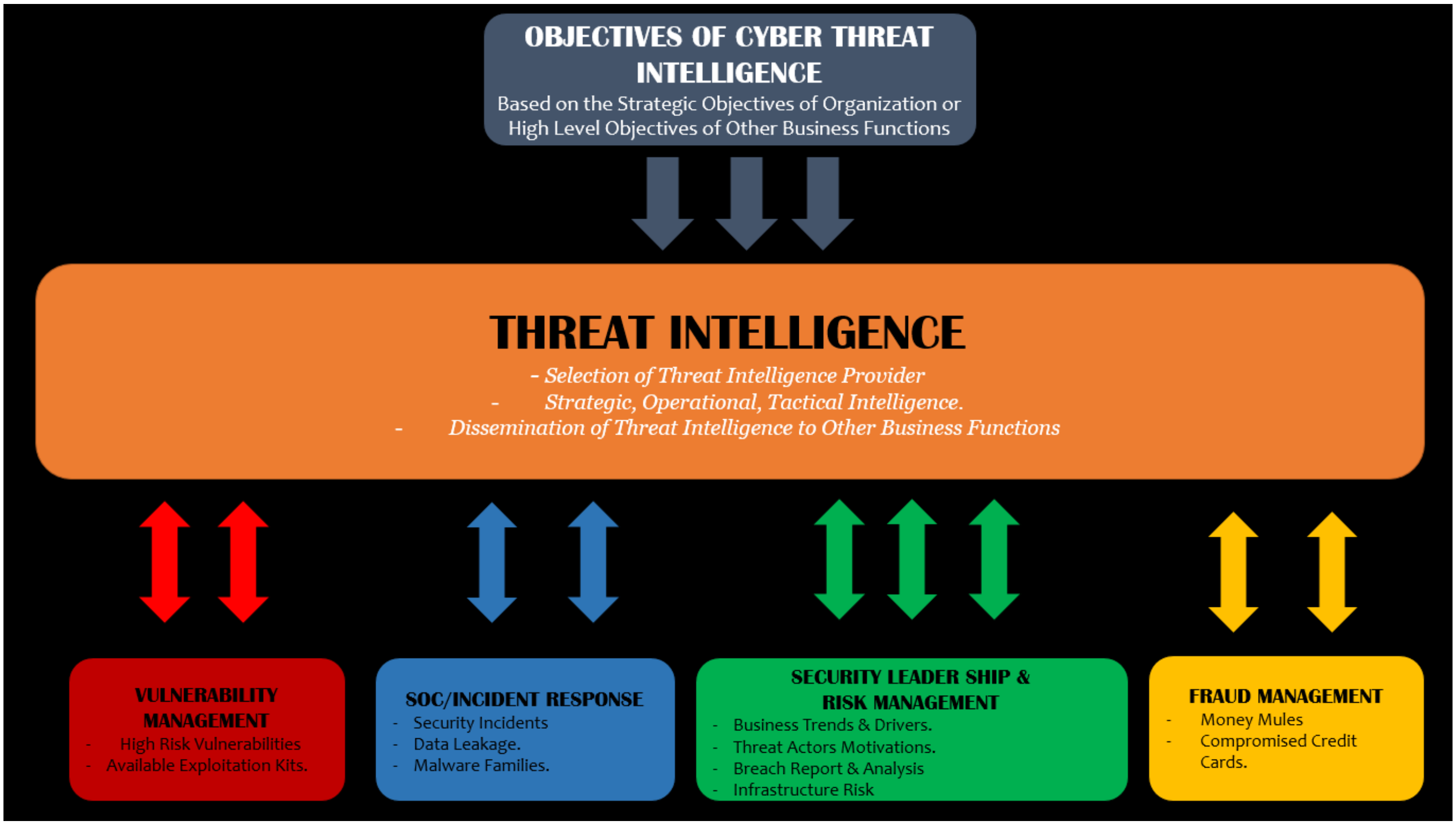
ESTABLISHING A CYBER THREAT INTELLIGENCE FUNCTION

I discussed at the start where Cyber Threat Intelligence stands in the broader canvas and its significance, however its establishment as an effective function demands consistent review, refinement and integration with other business functions.

Cyber Threat Intelligence acts essentially as the Main artery of the city through which the major chunk of the city traffic flows. The Main traffic artery of the city cuts across different secondary and tertiary roads to pour in or absorb traffic.

In the same capacity, Cyber Threat Intelligence holds other business functions of the organizations together, aiding them in informed decision making.

To begin with, the organization first needs to identify the business and security functions to be integrated with Cyber Threat Intelligence function, understand the strategic goals of the organizations or the goals of other business and security functions. This will help establish the goals for Cyber Threat Intelligence function, understand the intelligence needs and selection of appropriate Threat Intelligence Provider.


OBJECTIVES OF CYBER THREAT INTELLIGENCE
Based on the Strategic Objectives of Organization or High Level Objectives of Other Business Functions
THREAT INTELLIGENCE
- Selection of Threat Intelligence Provider
- Strategic, Operational, Tactical Intelligence.
- Dissemination of Threat Intelligence to Other Business Functions
VULNERABILITY MANAGEMENT
- High Risk Vulnerabilities
- Available Exploitation Kits.
SOC/INCIDENT RESPONSE
- Security Incidents
- Data Leakage.
- Malware Families.
SECURITY LEADER SHIP & RISK MANAGEMENT
- Business Trends & Drivers.
- Threat Actors Motivations.
- Breach Report & Analysis
- Infrastructure Risk
FRAUD MANAGEMENT
- Money Mules
- Compromised Credit Cards.

Let us dive in to discuss the purpose and the role of Cyber Threat Intelligence in each of these Business or Security Functions.

1. VULNERABILITY MANAGEMENT

Due to various business needs, IT teams are often compelled to punch holes in the Security stature with the purpose of enabling business needs. On the other hand, the Vulnerability Management teams are requesting the Patch Management teams to patch the vulnerabilities.

Patching all the vulnerabilities or closing any potential touchpoints for exploitation is a challenging task as it often pushes the Patch Management teams to the brink of breaking point and the real ugly battle begins when SLAs start getting impacted because the number of new vulnerabilities discovered every day are too much and the patch management is already under duress to patch previous stream of vulnerabilities.

Cyber Threat Intelligence helps the Vulnerability Management teams by shifting the focus from patching everything to making risk based decisions.

Since time is of essence for Vulnerability Management teams, therefore the goal should be to identify and address the threats most likely to be exploited against your organization. The Vulnerability Scanning Solutions are capable of scanning the organizational infrastructure against the list of vulnerabilities or specific vulnerabilities and populate the list of assets vulnerable. However there are some additional points that need to be considered after you've identified vulnerable assets.

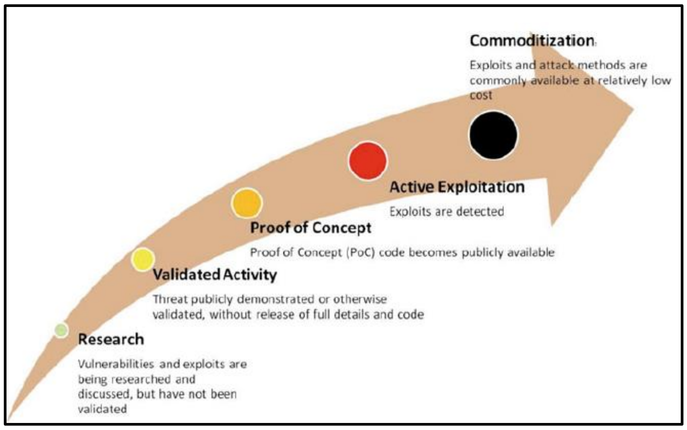
1. *Severity Ratings Do Not Represent Real Risk* - Ranking and classification schemes such as Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring Systems (CVSSs) don't factor in if threat actors are actually exploiting vulnerabilities right now in your industry vertical or region which means that vulnerability databases highlight technical exploitability, providing a verdict on the likelihood that exploitation of a particular vulnerability will result in specific magnitude of damage to systems and networks.

While a Vulnerability may have low CVSS score but can still pose a Real Risk derived due to active exploitation by cyber threat actors.

2. *Not Every Vulnerability Present in Your Environment Present Real Risk*

I referred to "*active exploitation*" as a factor in determining a Real Risk. The active exploitation is also dependent on the availability of the Exploitation Kits.

Intel Corporation presented a Product Life Cycle Model to tracking Evolution of Threats which shows that threats emerge as theoretical risks but progressively mature as their exploitability is demonstrated, their proof of concepts become publicly available and eventually their product are commoditized. With each subsequent stage the level of Real Risk increases and so does the potential for active exploitation.


Commoditization
Exploits and attack methods are commonly available at relatively low cost
Active Exploitation
Exploits are detected
Proof of Concept
Proof of Concept (PoC) code becomes publicly available
Validated Activity
Threat publicly demonstrated or otherwise validated, without release of full details and code
Research
Vulnerabilities and exploits are being researched and discussed, but have not been validated

Source Intel Corporation, 2012: Product Life Cycle Model - Tracking Evolution of Threats.

Threat intelligence provides information about the progression of a vulnerability, its active exploitation, Real Risk and empowers the Vulnerability Management Teams to work with their counterparts in Patch Management, prioritizing the patch implementations for vulnerabilities that pose significant risk.

Other benefits offered to Vulnerability Management include:

- *Providing actual Exploit Kits/PoCs to Penetration Testers in order to perform their Red Teaming activities to test a vulnerability exploitation.*
- *Providing insights like threat actor's interest and motivations linked to active exploitations of certain vulnerabilities.*

2. SOC/INCIDENT RESPONSE TEAM

Security Operations & IR Teams are usually the consumers of Tactical and Operational Intelligence as they serve the function of ears and eyes of the entire Organizational Infrastructure from Security lens.

Security Operations need to understand the high level objectives of other business and security functions. This understanding is essential because every Strategic Intelligence has its Operative & Tactical part which needs to be consumed and acted upon to establish or maintain detective, preventative and corrective controls which eventually maintain the Security Hygiene and secure Posture of the Organization.

One of the major challenges faced by Security Operations is the alert fatigue caused by the huge volume of alerts created by various network entities. It pushes Security Operations to often chase ghosts, miss out on important alerts and largely cultivate a reactive approach and mentality.

Tactical Intelligence for the SOC, enriches the internal alerts with external information and context necessary for triage, scoping and containment actions. Operational Intelligence helps the Security Operations to understand the Cyber Threat Landscape, threat vectors that pose greatest risks and the common tools, tactics, techniques and procedures used by Threat Actors to target their Industry or region.

2.1 MEASURING DEFENSE CAPABILITIES AGAINST ADVERSARIES

To determine & measure Defense Capabilities against determined Cyber Threat Actors, I recommend the following steps.

1. Identify the adversaries to determine and measure your defense capabilities against.

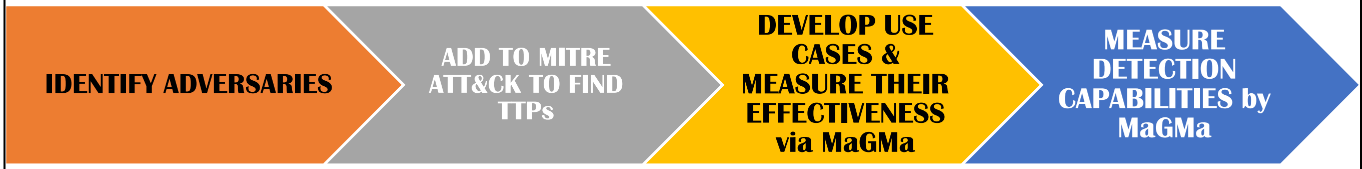
2. Incorporate MITRE ATT&CK Navigator tool to help you identify the TTPs for specific adversarial groups targeting your Industry or region.

MITRE ATT&CK Navigator tool helps you adopt a Risk Based approach based on the shared TTPs among all Threat Actors that you have identified

3. **Incorporate MaGMa Use Case Framework developed by Dutch Payment Associations**

The MaGMa Use Case Framework is a very effective tool to measure your detection capabilities and allows you map your technical Use Cases to Strategic goals. MaGMa Use Case Framework has all its suggested Use Cases tied to specific MITRE ATT&CK TTPs.

This establishes a complete Risk driven mechanism to help the Security Leadership have a solid understanding of their defense capabilities and identification of areas where risk levels are heightened and where resources are required for risk optimization.


IDENTIFY ADVERSARIES
ADD TO MITRE ATT&CK TO FIND TTPs
DEVELOP USE CASES & MEASURE THEIR EFFECTIVENESS via MaGMa
MEASURE DETECTION CAPABILITIES by MaGMa

Cyber Threat Intelligence also helps the organizations in identification of any organizational data which is available for sale on Deep and Dark Web.

2019 Cost of a Data Breach Report mentioned that on an average it took organizations 279 days to detect a Data Breach which is more than 9 months, this is an enormous time to detect any data breach and by the time an organization detects the Data Leakage or Breach, the data may have already proliferated across various threat actors which makes the Senior Management unable to accurately ascertain the Risk Level and respond appropriately.

3. SECURITY LEADERSHIP & RISK MANAGEMENT

Before we highlight the needs that the Chief Information Security Officer, Chief Security & Privacy Officers may have for Cyber Threat Intelligence, let's understand challenges that these C-Level executives are embattled with.

The Chief Security Professionals are primarily responsible for enacting high level policies and mechanisms that establish and maintain a Secure Posture to enable the organization seek and attain its mission, goals and objectives. This challenge is often exacerbated due to tight financial budgets because implementation of Security by itself does not reap monetary benefits.

These challenges require a thorough understanding of the risk spectrum and intelligent allocation of budgets to relevant risk response options.

The function of Risk Management is main ammunition in the armory of security leadership where business, technical, digital, reputational risks etc. are identified and estimated and subsequently their risk treatment options are determined.

Though audit findings are helpful in identification of risks in the Security posture and are factored in the Risk Assessment, however these findings are mostly centered on existing Security best practices and are not aware of the new techniques employed by cyber threat actors, evolution of threats, emerging trends and drivers that can create Security Risk.

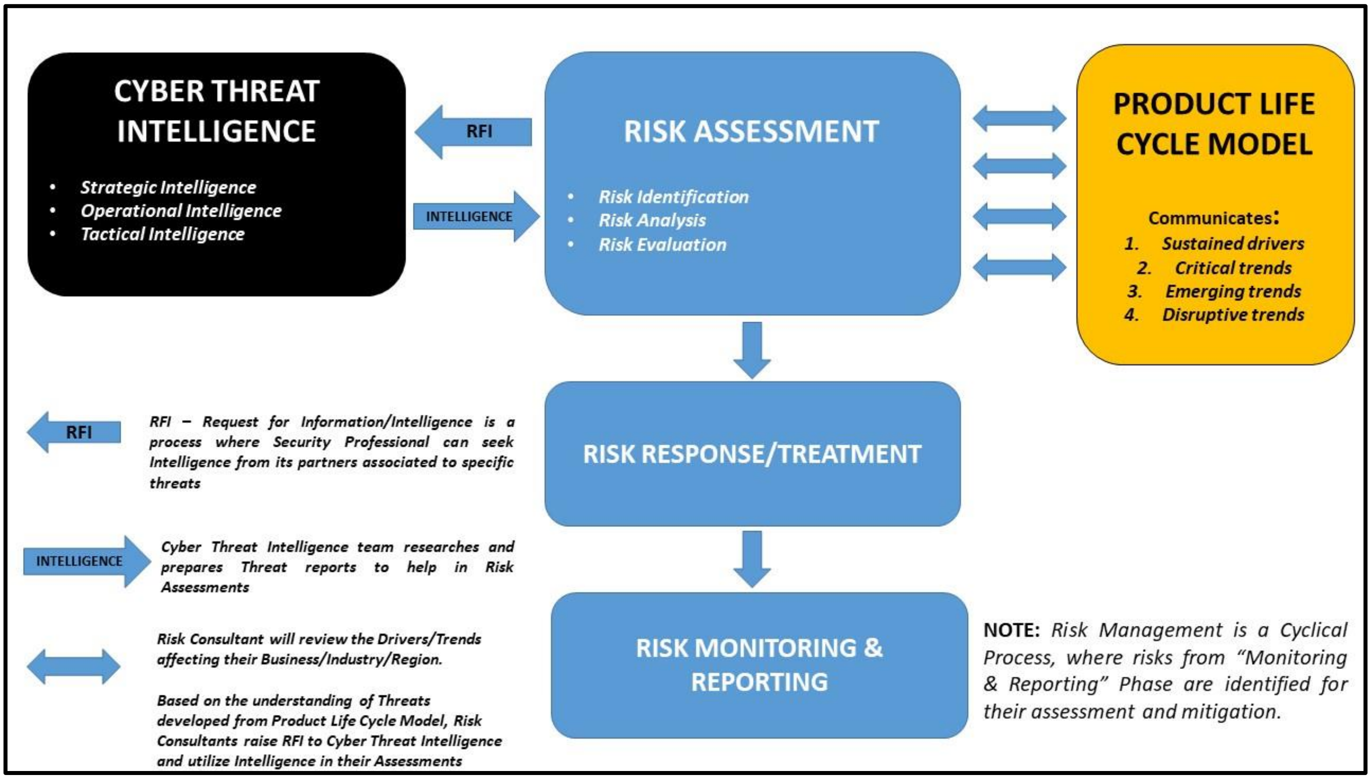
This tends to raise a question on the overall efficacy of the Risk Management function where Risk Spectrum does not accurately reflect and deal with threats related to business trends.

In one of my earlier paper, I've mentioned how incorporating Intel's Product Life Cycle Model on Evolution of Threats can help the Security Leadership understand the trends and the associated threats.

Trends/Drivers	Description	Examples
Sustained drivers	Areas that already have a high impact or otherwise cause considerable concern.	Malware and Web attacks.
Critical trends	Areas that have begun undergoing active exploitation, with growing adoption beginning to shift toward commoditization.	Social computing & Smartphones
Emerging trends	Areas that have a low current level of exploitation, but considerable research and proof-of-concept activity	Embedded & Cloud Computing
Disruptive trends RISK	Areas with little or no active exploitation, but significant research activity and the disruptive Potential to cause a major security problem. Frequently, they are discussed as theoretical risks, and because of this, many people in the industry would be caught off guard by a significant event.	Virtualization

Source Intel Corporation, 2012: Product Life Cycle Model - Tracking Evolution of Threats.

Once these threats and their evolution is understood, it helps the Security Leadership demand for relevant Strategic Intelligence. Having an Actionable Strategic & Operational Threat Intelligence strengthens Risk Management functions in correct identification of Risk Scenarios and can also aid in the process of Risk Estimation.



RFI – Request for Information/Intelligence is a process where Security Professional can seek Intelligence from its partners associated to specific threats

Cyber Threat Intelligence team researches and prepares Threat reports to help in Risk Assessments

Risk Consultant will review the Drivers/Trends affecting their Business/Industry/Region.

Based on the understanding of Threats developed from Product Life Cycle Model, Risk Consultants raise RFI to Cyber Threat Intelligence and utilize Intelligence in their Assessments

NOTE: *Risk Management is a Cyclical Process, where risks from "Monitoring & Reporting" Phase are identified for their assessment and mitigation.*

This entire process enables the Security Leadership and Risk Management Function to accurately understand risk spectrum, develop appropriate strategies to deal with identified risks and justify the required investments in security apparatus with the overall objective to establish and maintain Secure Posture to enable the organization seek and attain its mission, goals and objectives.

4. FRAUD MANAGEMENT

We shall in coming sections see how underground market is structured in terms of its offerings. Understanding of the Underground market and communities can help us ascertain the risks associated with specific sightings (*in terms of chatter, sale of access, data etc*.)

4.1 Financial Sector is subjected to compromised payment data which can be collected by threat actors through a multitude of avenues including phishing, web sniffers etc. Such card data and its dumps are often sold by threat actors and are available for purchase at different underground shops.

Intelligence related to Cards Data getting traded on underground forums and various shops, provides insight on the value of your cards and the potential loss due to fraudulent transactions due to exposure of such data, it can allow risk management function to evaluate the cost associated with the re-issuance of new cards to their customers.

4.2 Creation of phishing domains & cybersquatting is another aspect where Threat Intelligence aids the Fraud Management process. Phishing Domains misrepresenting organizations' official domains; are often the precursor to a cyber-attacks therefore any proliferation of such domains help the organization to review and understand the threat landscape and subsequently take down such domains before they are exploited by threat actors to cause harm to organizational reputation.

4.3 Executive Impersonation is another aspect where Cyber Threat Intelligence helps the organization to identify and flag any fake profiles of senior executive management on the social media channels. These channels can be leveraged by the cyber threat actors to spread fake news, fake promotions, or divert users to malicious channels by first associating their own profiles with the organization.

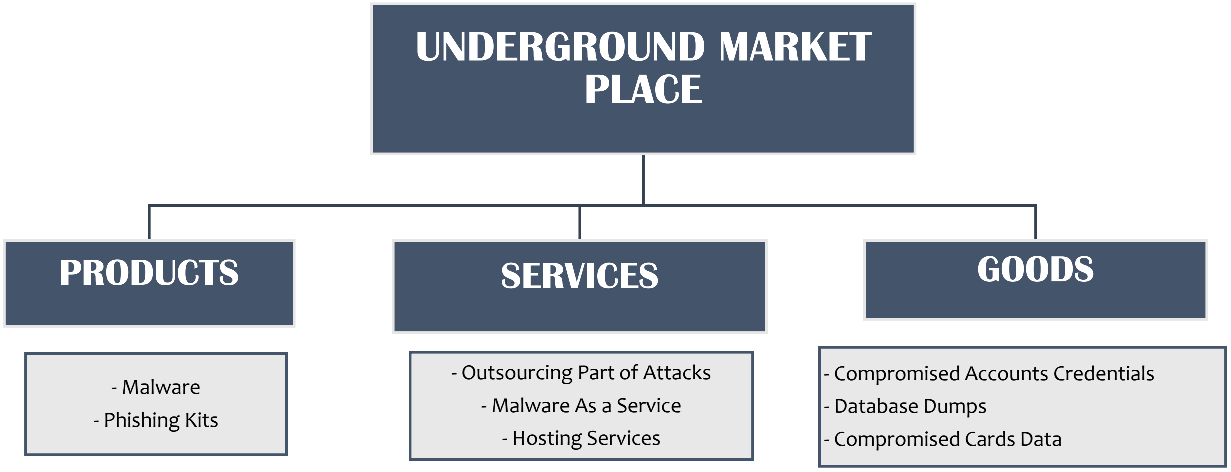
Timely identification of these profiles help the organization to take down similar fake profiles impersonating senior executives and causing reputational damage.

UNDERSTANDING CYBER UNDERGROUND MARKET

Cyber Underground marketplace is fundamentally similar to any other market place in a normal society. In any society the concept of market place is that of an area where people meet to buy and sell goods, products and services.

In a similar manner, cyber underground market is a place where various threat actors meet to buy or sell the goods, products and services which can be leveraged by various groups and threat actors in their attack campaigns to carry out their targeted attacks. The access to such market sites is usually open and does not require an existing member to vouch for new entrants.

Intel 471, A Cybercrime Threat Intelligence Provider has wonderfully visualized this arrangement (redrawn version given below) of cyber underground market.



It also alludes to the fact that cyber-attacks are rarely carried out by individuals operating in isolation but mostly carried out through a well-coordinated campaigns to serve the end goal.

In a conventional attempt to physical sabotage, destruction or terrorism; it has been seen that various gangs or opportunistic criminals lend their services and support to bigger criminal syndicates, acting as their accomplices and aiders.

In a similar manner advanced cyber-attacks require varying levels of skills, infrastructure and tools and involve various stages to achieve their end goal. Threat Actors therefore work in tandem based on each other's strengths, offerings and geographical location and utilize different products, services and goods based on their campaigns and motivations.

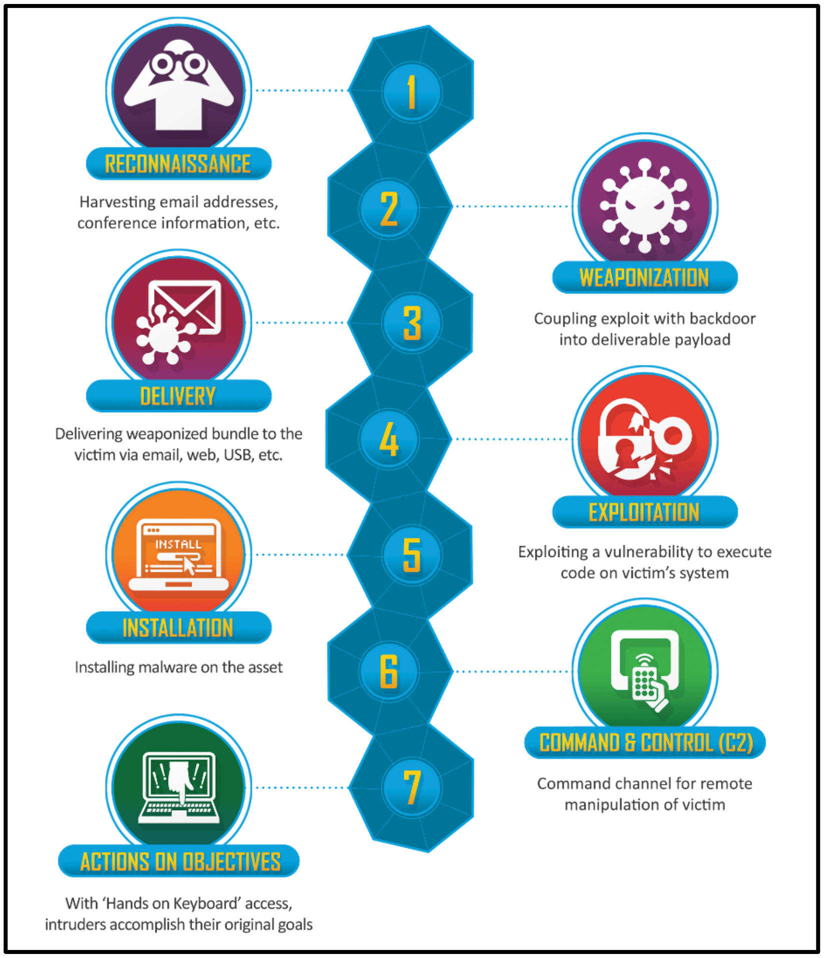
It is also vital to establish a clear distinction here between Deep & Dark Web as these nomenclatures are often used interchangeably.

DEEP WEB	**DARK WEB**
Web Areas not indexed/reached via search engines	Areas accessible on via special software/tools that mask visitors' identity.

This understanding of cyber underground market is pivotal to be understood by the consumers of Cyber Threat Intelligence as it equips them to understand the threat actors' motivations, predict their objectives, and understand their collaborations and the motivations behind those collaborations.

Such invaluable contextual information & understanding puts the organizations and Security Professionals ahead of their adversaries by first helping them understand the evolution of threats *(whether the attack is still being planned by acquisition of necessary tools, collaborations forged, initial probing attempts seen) and* subsequently fortifying their defenses proportionately.

Security Operations or Incident Response Teams can benefit a great deal by mapping out this intelligence on cyber kill chain and correctly understanding the intent, capabilities of threat actor and progress made in carrying out the attack.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Lockheed Martin, Cyber Kill Chain Framework

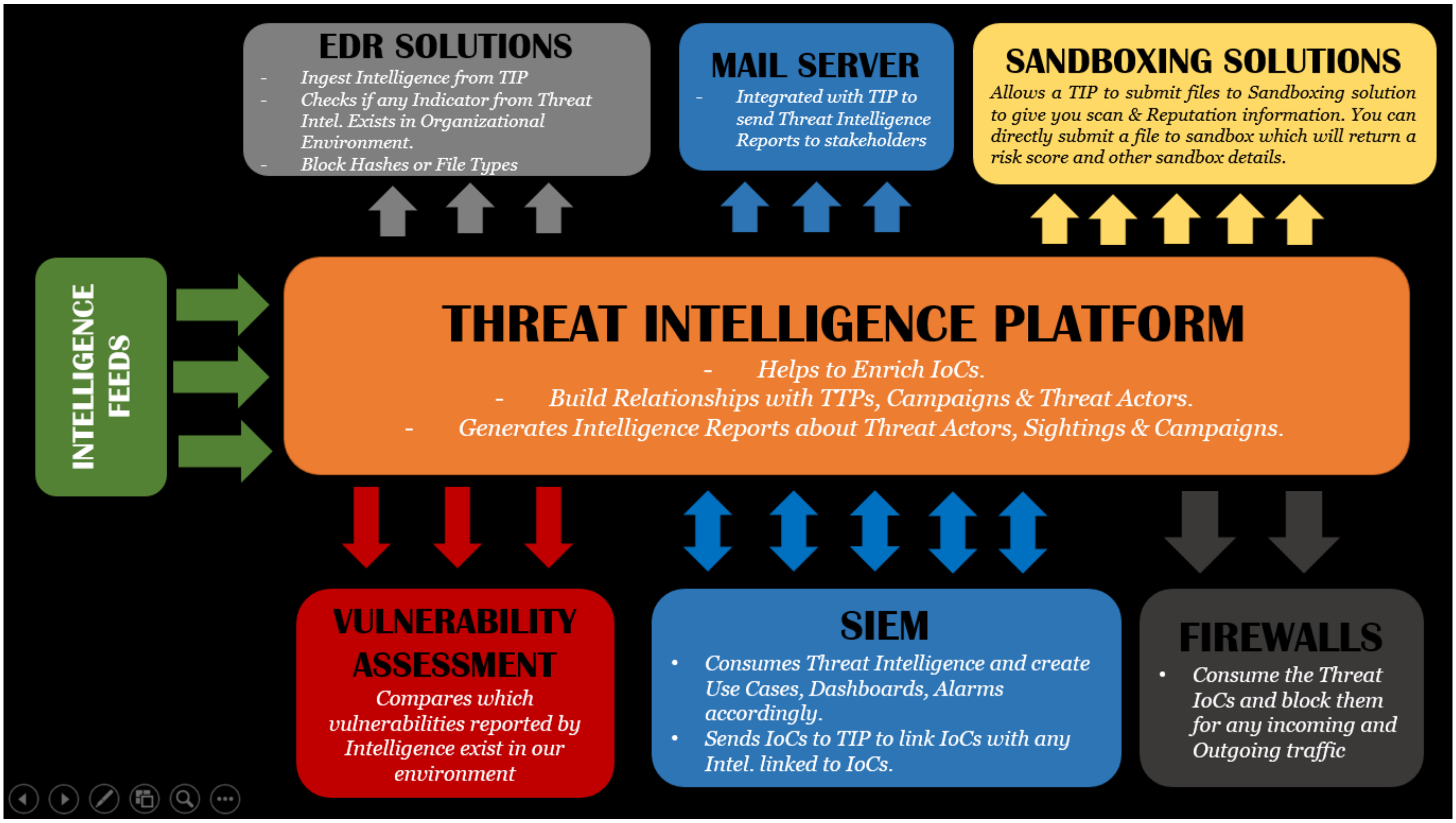
THREAT INTELLIGENCE PLATFORM INTEGRATIONS WITH OTHER SECURITY SOLUTIONS

Now that we've elaborated on the Cyber Threat Intelligence, its consumers and the kinds of Intelligence along with the establishing the understanding of cyber underground market, let us proceed to discuss the framework of integrations around your threat intelligence platform.

As you understand your intelligence needs and subscribe to a different sources of Cyber Threat Intelligence, a platform is needed to gather, store, process and search the information.

Threat-intelligence platform (TIP) is essentially a database housing the threat information. It is imperative that your Threat Intelligence Platform is integrated with various other Security Devices like Firewalls, SIEM, Vulnerability Management tool, Sandboxing tools, in your organization to avoid it function in a silo. These integrations create an environment for collaboration among different sub functions of information security and make the task of your security operations team easier and guard them against alert fatigue.

Please refer to below, demonstrating the *framework of integrations* that I propose around threat intelligence platform. Some of these integrations may be limited to threat intelligence platform capability to integrate with other security solutions while some may offer other integration capabilities as well like that of Integration with Exchange Server & Active Directory to pull in the Emails from Mailbox and having a copy of Active Directory Identities in TIP, however I would caution against integrating these entities with TIP without engaging your data governance and protection teams since it can create Privacy issues for users whose emails are fed intelligence platform.



EDR SOLUTIONS

- *Ingest Intelligence from TIP*
- *Checks if any Indicator from Threat Intel. Exists in Organizational Environment.*
- *Block Hashes or File Types*

MAIL SERVER

- *Integrated with TIP to send Threat Intelligence Reports to stakeholders*

SANDBOXING SOLUTIONS

Allows a TIP to submit files to Sandboxing solution to give you scan & Reputation information. You can directly submit a file to sandbox which will return a risk score and other sandbox details.

INTELLIGENCE FEEDS

THREAT INTELLIGENCE PLATFORM

- *Helps to Enrich IoCs.*
- *Build Relationships with TTPs, Campaigns & Threat Actors.*
- *Generates Intelligence Reports about Threat Actors, Sightings & Campaigns.*

VULNERABILITY ASSESSMENT

Compares which vulnerabilities reported by Intelligence exist in our environment

SIEM

- *Consumes Threat Intelligence and create Use Cases, Dashboards, Alarms accordingly.*
- *Sends IoCs to TIP to link IoCs with any Intel. linked to IoCs.*

FIREWALLS

- *Consume the Threat IoCs and block them for any incoming and Outgoing traffic*

OTHER PROTOCOLS

Traffic Light Protocol is the current standard for sharing threat intelligence data and contains following levels.

TRAFFIC LIGHT PROTOCOL (TLP)	DESCRIPTION
TLP: RED	Restricted – Not for Sharing
TLP: AMBER	May Only share information with Members of the Organization
TLP:GREEN	May Share Information with Peers & Partner Organizations
TLP: WHITE	Publicly available information – Can be Shared with Anyone.

TAXII (Trusted Automated exchange of Intelligence information)

TAXII is the protocol for transport & exchange of Threat Intelligence. It supports information represented in STIX format.

STIX (Structured Threat Information Expression)

STIX is a format that carries the threat information from one party to another meaning that data such as Malware Hashes, FQDNs, and Indicators of Compromise etc. are shared between the parties in STIX format but are transported over TAXII.

STIX and TAXII, together enable the sharing of threat intelligence in a secure manner between the parties willing to exchange intelligence.

CHALLENGES RELATED TO THREAT INTELLIGENCE INGESTION

Some of the challenges while utilizing Threat Intelligence & Threat Intelligence Platform are mentioned below and must be attended to carefully in order to fully operationalize and maximize the benefits of threat management function.

1. *Lack of Actionable Intelligence from Threat Intelligence feed Providers.*

2. *Interoperability issues with specific Threat Intelligence Platforms.*

3. *Not All Intelligence provided by Intelligence providers is sent to Threat Intelligence Platforms due to nonexistent APIs.*

4. *Threat Intelligence Platforms are unable to properly parse the Intelligence received in STIX/TAXII format into their respective categories/objects/indicator fields.*

5. *Threat Intelligence Platforms do not support specific integrations with other Security solutions like Email Filtering Solutions, Firewalls, SIEM, Vulnerability Management solutions etc.*

6. *Threat Intelligence Platforms must enable teams to perform investigations and build relationships among low level IoCs, TTPs and their adversaries.*

7. *Threat Intelligence Platforms must have a reporting function to send periodic or ad-hoc reports to stakeholders.*

RELATIONSHIP BETWEEN THREAT INTELLIGENCE AND THREAT HUNTING

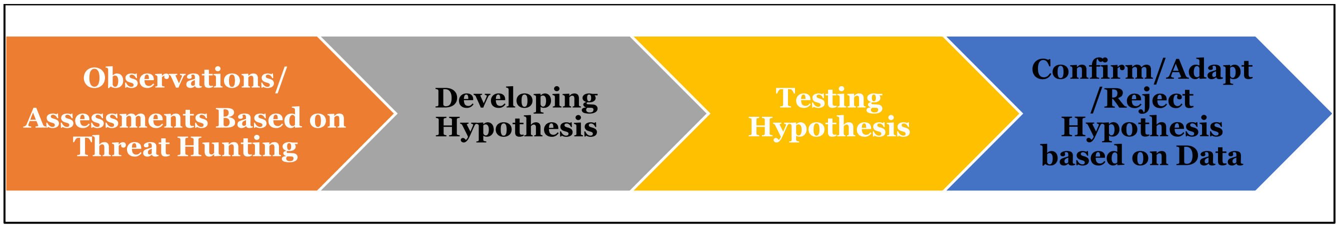
Threat Intelligence equips Threat Hunting exercises by providing Security Operations, the intelligence with leads to perform further excavation of threats that may be lying beneath the surface.

The Threat Hunting process can be triggered by a multitude of inputs that can come either through Threat Intelligence highlighting the adversarial campaigns, selling of specific malwares or other services etc. or it can be triggered through certain anomalous sightings in network traffic, user behavior or network scans.

THREAT INTELLIGENCE
DRIVES
THREAT HUNTING

While performing hunting exercise, threat intelligence can be used for similar Tactics, Techniques and Procedures to understand the potential adversary behind the attack and the campaign it might be related to. MITRE ATT&CK framework can be invaluable in this regard.

Such steps can be used to drive the further iterations of the hunt which leads to refinement of hypothesis or generating ideas for later hunts.


Observations/ Assessments Based on Threat Hunting
Developing Hypothesis
Testing Hypothesis
Confirm/Adapt /Reject Hypothesis based on Data

After various iterations of Threat Hunting, the teams develop a number of hypothesis which need to be tested.

Below are some of the characteristics of good hypothesis:

1. *Should Be Clear & Concise.*
2. *Able to be tested within a reasonable time and should have a specific scope.*
3. *Should be based on Observables – a good hypothesis is based on the events observed suspected to lead to an incident and should not be based on wild guesses.*

Once hypothesis is put forward based on the characteristics mentioned, the next stage is to validate the hypothesis.

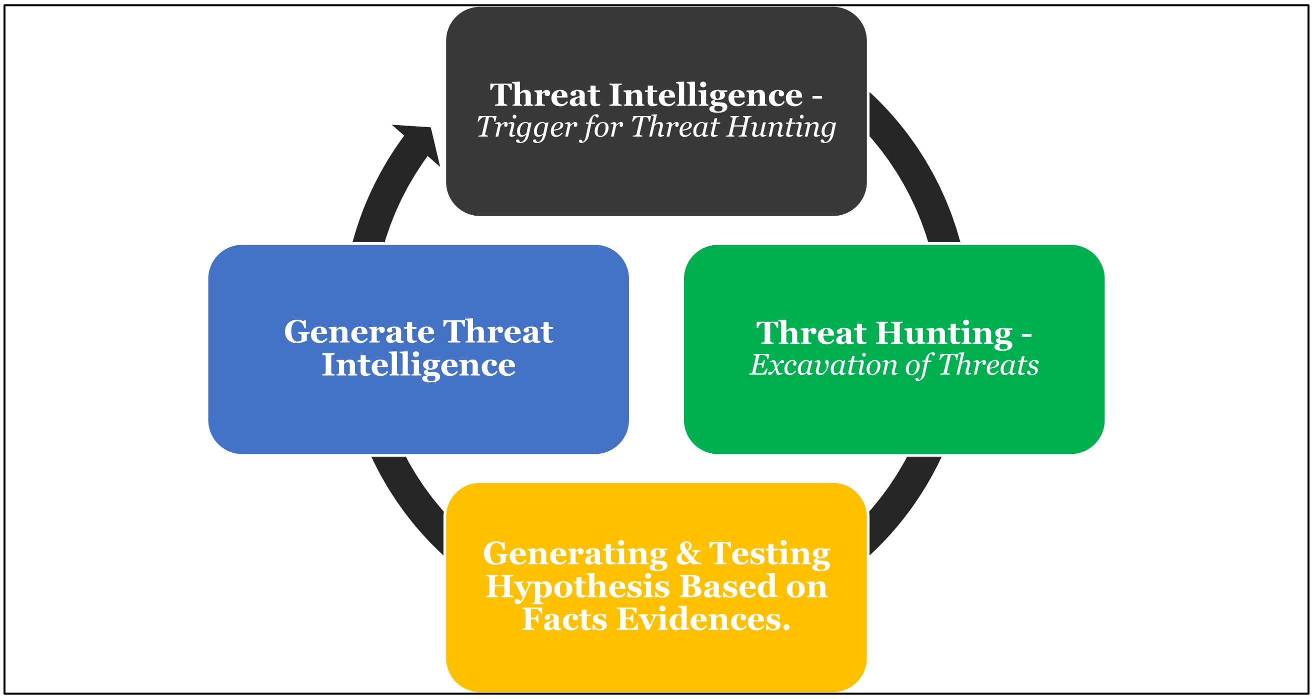
Gathering your evidences to substantiate your conclusion over hypothesis is extremely important and requires threat Analysts to be mindful of specific biases they may be victim to and eventually lead to incorrect conclusions. Some of the biases to fight while performing Threat Hunting are mentioned below:

1. Confirmatory Bias: Threat Hunters look for specific angles, evidences or behaviors from the entire threat spectrum to prove their hypothesis which is not consistent with what the evidences communicate.

2. Anchoring Bias: Threat Hunters rejection of emerging information keep them hooked to their earlier conceived hypothesis which is in complete contrast to very fundamental concept of Threat Hunting being an Iterative exercise.

3. Selective Bias: Reaching to specific conclusion based only the data available rather than the full range of data to test the hypothesis.

Adoption of Approaches mentioned above lead to generation of threat intelligence. As Threat teams hunt, they uncover unknown TTPs for attackers which can be used to map to adversaries. Such information can then be shared as threat intelligence in ISACs and other communities, providing them with information regarding the uncovered threat. If the peers in community begin their own hunting exercise based on this new TTP, they can further uncover additional indicators of attack that can be shared as threat intelligence with community.


Threat Intelligence - *Trigger for Threat Hunting*
Threat Hunting - *Excavation of Threats*
Generating & Testing Hypothesis Based on Facts Evidences.
Generate Threat Intelligence

CONCLUSION

An Effective Cyber Threat Intelligence function identifies unknown threats, provide better understanding of Risk Spectrum and enhances the overall effectiveness of Information Security Divisions.

APPENDIX: List of Acronyms

BoD	Board of Directors
TTP	Tactics, Techniques and Procedures
SOC	Security Operations Center
PoC	Proof of Concept
IoC	Indicators of Compromise
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
ATT&CK	Adversarial tactics, techniques, and common knowledge
MaGMa	Management, Growth, Metrics & Assessment.
TIP	Threat Intelligence Platform
FQDNs	Fully Qualified Domain Names
SIEM	Security Information and Event Management

REFERENCES

MITRE ATT&CK:

https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

https://medium.com/mitre-attack/using-att-ck-to-advance-cyber-threat-intelligence-part-2-6f21fdba80c

https://attack.mitre.org/resources/getting-started/

https://www.youtube.com/watch?v=pcclNdwG8Vs&feature=youtu.be

MaGMa Use Case Framework

https://www.betaalvereniging.nl/en/safety/magma/

https://www.recordedfuture.com/threat-intelligence-data/

Deep & Dark Web

https://medium.com/digital-marketing-lab/the-difference-between-the-deep-web-and-the-dark-web-ec5a94b3655f

https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11

https://www.youtube.com/watch?v=Ow4LvwpqTtc

https://www.youtube.com/watch?v=fUjSVrh9UN4

STIX/TAXII & TLP

https://www.us-cert.gov/tlp

https://www.anomali.com/resources/what-are-stix-taxii

Intelligence Types, Its Consumers & Veracity

Intelligence Driven Incident Response – 2nd Edition by Scott J. Roberts & Rebekah Brown

https://www.splunk.com/en_us/data-insider/operational-intelligence.html

https://www.recordedfuture.com/operational-threat-intelligence/