Telefónica Tech

This report is offered by celcom business

NextDefense

CHAPTER 1

Sailing through the *Threat Intelligence* Vendor ocean

1 About the Research

Nikolaos Tsouroulas is the Global Product Management Manager for MSS, MDR and Threat Intelligence at ElevenPaths, the cyber security team of Telefónica Tech.

For the last 18 years he has developed his career in the telecommunications sector, holding various research, engineering and management positions at British Telecom and Telefónica, always focused in the digitisation of the telecoms business projects and areas. His fields of experience and expertise cover mobile network optimisation, mobile devices and operating systems, cloud computing, information security, mobile security, network security, threat intelligence, managed detection and response and cyber security in general.

In his current role, he is responsible for defining and developing new managed cyber security services that go beyond the traditional perimeter-based defence paradigm, shifting the focus to prevention, detection and response. He works on finding ways to leverage threat intelligence, data analytics and innovative security approaches to develop products and services that protect not only an organisation's IT infrastructure, but also business processes and assets exposed on the Internet.

Contact:

nikolaos.tsouroulas@telefonica.com

LinkedIn | Nikolaos Tsouroulas

Collaborators:

Miguel Angel de Castro and **Ramiro Céspedes**

2 Executive Summary

During 2020, to expand Telefonica Tech NextDefende Detection and Response services the Threat Intelligence Unit was required to create a Threat Intelligence Product & Service Portfolio, by conducting Proof of Value (PoV) of several Threat Intelligence vendors' products and services. The PoV were performed by engineering a new evaluation methodology and framework that allowed the team to benchmark the vendors' Threat Intelligence **platforms capabilities** and its intelligence products' **quantity** and **quality**.

This is the first chapter of a two-chapter article in which we will be sharing the results and findings of our evaluations.

This first chapter is intended to educate the organizations and decision-makers by reviewing basic intelligence analysis concepts that will allow the reader to understand how Cyber Threat Intelligence (CTI) has its foundations in traditional intelligence analysis and how it can help an organization to improve its security posture.

2.1. Key Findings

- Education remains paramount. MSSPs (Managed Security Services Providers), MDRs and Cyber Threat Intelligence (CTI) vendors play a key role in this regard. Educating the organizations and key stakeholders such as CISOs on what is CTI and what is not, is beneficial for the organizations and also for the vendors since education can help their customers to understand what they are buying and align its expectations accordingly.
- In simple terms, we can define *Intelligence* as information that can be acted upon to modify certain outcomes.
- It is important to understand the **Intelligence Analysis Cycle** since it provides a framework and guide for intelligence teams to answer the Intelligence Requirements.
- The **Planning** phase of the **Intelligence Cycle** is critical for the success of any intelligence operation. In this phase is where **Priority Intelligence Requirements** (PIRs) and Information Requirements (IRs) should be defined so that the team has a clear understanding of which are the needs for intelligence and how will these needs be satisfied.
- Cyber Threat Intelligence is data that is collected, processed, analyzed, and disseminated.
- CTI products and services should help to understand a **threat actor's** motives, behavior and targets and to allow the organization to move from a reactive security approach to a proactive one.
- The organizations should focus on **who** (threat actor), **how** (Tactics, Techniques and Procedures) and **why** (motivation) could the organization be a target of a cyber-attack. Therefore, it is very important to understand the nature of the organization's business activities and the **context** it operates in (industry, region, countries, geopolitics).
- CTI can help the organization to move from Unknown Unknowns to Known Knowns by reducing uncertainty and improving decision-making.
- CTI products and services will also allow the organization to understand better the threat

landscape, to reduce MTTD (Mean Time To Detect) and MTTR (Mean Time To Respond) to security incidents.

- There are different CTI subtypes. These are Strategic, Operational, Tactical and Technical. The last 2 will often be combined in a single subtype. Each intelligence subtype is oriented to different consumers and has different objectives.

- Intelligence Collection methods (OSINT, HUMINT, SIGINT, etc) should not be mistaken as **CTI subtypes** since these are only methods of getting the raw information, which is needed to produce a finished intelligence product.

3 Talking about intelligence

To start with, we would like to define and be clear about what is *Intelligence* and what it is not. We are going to do so by explaining traditional intelligence analysis concepts that will allow us to understand how intelligence can be used in the cyber space.

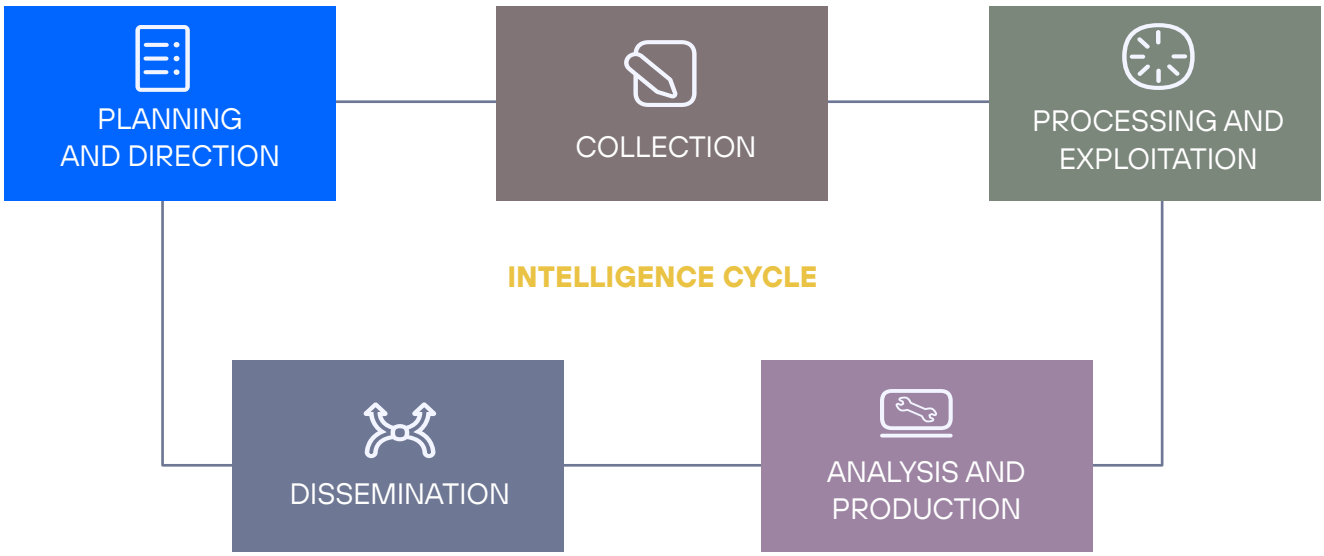
According to the Federal Bureau of Investigation (FBI), Intelligence is:

> ***"Information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security".***

To put it in other words, Intelligence is information that can be acted upon to modify outcomes, i.e., actionable information to help decision makers in addressing threats to their organization's assets.

3.1. The intelligence cycle

Intelligence is a finalized product that is created by the following process:



Planning and Direction

The phase is critical for the success of any intelligence operation. In this phase is where **Priority Intelligence Requirements** (PIRs) and **Information Requirements** (IRs) should be defined so that the team has a clear understanding of which are the needs for intelligence and how will these needs be satisfied.

What is an Information Requirement?
Those items of information regarding the adversary and the environment that need to be collected and processed in order to meet the intelligence requirements of a stakeholder.
Source: https://www.militaryfactory.com/dictionary/military-terms-alphabet-list.asp?letter_group=I

What is a Priority Intelligence Requirement?
Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence.
Source: https://www.militaryfactory.com/dictionary/military-terms-alphabet-list.asp?letter_group=I

Collection

The collection phase involves gathering raw information from different intelligence sources that will be used to produce the finished intelligence product. There are different collection methods such as:

- **OSINT** *(Open-Source Intelligence)*: Publicly available information appearing in print or electronic form, including radio, television, newspapers, journals, the Internet, commercial databases, videos, graphics, and drawings. Something very common nowadays is to obtain intelligence from social network profiles or open communication channels.
- **HUMINT** (*Human Intelligence*): Intelligence derived from human sources and collected openly or covertly (espionage). For example, intelligence analysts infiltrated in underground forums and communication channels that are able to interact with the different threat actors.
- **MASINT** (*Measurements and Signatures Intelligence*): Scientific and technical intelligence information used to locate, identify, or describe distinctive characteristics of specific targets. It is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities.
- **SIGINT** (*Signals Intelligence*): The interception of signals, whether between people, between machines, or a combination of both.
- **IMINT** *(Imagery Intelligence)*: Representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.
Fuente: https://usnwc.libguides.com/c.php?g=494120&p=3381426

Processing and Exploitation

This phase is where the analyst will filter and synthesize all the raw collected data to make it ready for exploitation. With this, the analyst will be able to validate the collected data to determine its relevance and usefulness.

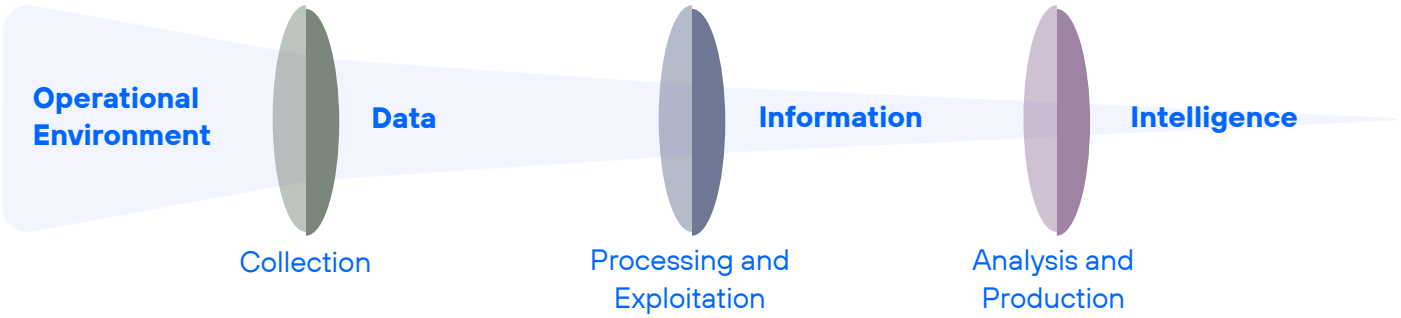
Analysis and Production

It involves the integration, evaluation, and analysis of the raw data to convert it to a finished intelligence product.

Dissemination

It is where the intelligence product is distributed in the proper digestible format to the stakeholders who requested it.

Relationship of Data, Information and Intelligence:



3.2. What is Cyber Threat Intelligence?

Now that we have seen and understood traditional Intelligence Analysis concepts let's define what is Cyber Threat Intelligence. Gartner defines Threat Intelligence products and services as:

> ***"evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard".***

To expand on Gartner's definition, we can say that CTI is product dependant on a clear process. CTI is data that is collected, processed, analyzed, and disseminated. Its final product, actionable information, should serve to understand a **threat actor's motives, behavior and targets** and therefore to allow the organization to move from a reactive security approach to a proactive one.

In other words, Cyber Threat Intelligence should help an organization to understand their Threat Landscape and address those threats accordingly.

Moreover, Threat Intelligence products and services will also allow the organization to understand better the threat landscape, to reduce MTTD (Mean Time To Detect) and MTTR (Mean Time To Respond) to security incidents.

3.3. Cyber Threat Intelligence subtypes

We have often seen misunderstandings when defining what is Cyber Threat Intelligence and which are the different intelligence subtypes which **are not** the same as **intelligence collection** methods. For example, OSINT is not CTI. OSINT is one collection method use in CTI to develop the finished intelligence product.

We can divide Cyber Threat Intelligence into 4 different subtypes. These are different in terms of the timeframe the product is valid, who is the consumer, which is the main objective and how it is consumed.

Intelligence Type	What is it	Who is the consumer	What is the objective	What is the Intel product
Strategic	High level and long-term information.	Board level, senior decision makers or staff reporting to the board.	Understand risks and likelihood of the threat landscape.	Reports about financial impact of cyber activity, attack trends on specific industries or regions and other matters that may impact high-level business decisions.
Operational	High level and short-term Information.	High-level security staff.	Prevent and mitigate attacks.	Reports about adversaries and their campaigns that will likely target the organization for any specific reason. Information about attacks with identity (when attribution is possible) and capability of the adversary.
Tactical	Low level and long-term information.	CERT and Defenders.	Understand how the adversary will attack the organization and adjust the defenses accordingly.	Attacker methodologies, their tools and tactics, techniques, and procedures (TTPs).
Technical	Low level and short-term information.	Security Platforms and Tools (Firewall, SEG, SIEM, EDR, TIP, SOAR, etc).	Automate blocking of suspicious or compromised infrastructure.	Malware and intrusion Indicators of compromise (IOCs) that are linked to the adversary infrastructure or tools.

4 The Cyber Threat Actor Ecosystem

We have seen how important it is to understand that Cyber Threat Intelligence has to do with the **threat actors** and with **how** (Tactics, Techniques and Procedures) and **why** (motivation) are they likely to target our organization. Therefore, it is very important to understand the nature of the organization's business activities and the **context** it operates in (industry, region, countries, geopolitics).

Cyber Threat Actors are not equal in terms of motivation, sophistication, and capabilities. Considering these attributes, we can classify Threat Actors as the following:

Type	Motivation	Sophistication	Target	Affiliation
Cyber Criminals	Financial Gain.	Medium.	Data, Personal Identifiable Information (PII) or Intellectual Property (IP) that can be hold for ransom or auctioned if the victim does not pay the ransom.	Individual or other cybercriminal groups.
Hacktivists	Ideological, to promote a political agenda or social change.	Low.	Government agencies, multinational organizations.	NGO or individuals.
Cyber Terrorists	Ideological, Financial gain, Propaganda, Reputation.	Low.	Nation-State, organizations.	Terrorists groups.
Insider	Financial Gain, Revenge.	Dependent on the access level.	Intellectual Property, System and Network Access.	Any.
Nation-State	Geopolitical, Espionage.	High.	High profile nation-state organizations or strategic industry organizations.	Cybercriminals or other nation-state sponsored groups.

Although we can categorize and separate threat actors this does not mean that threat actors do not collaborate and do business between themselves. For the last years, we have started to see how the cybercriminal ecosystem has been evolving to become a mature business model where providers and customer can perform safe business transactions. It is normal to see malware developers in what is in commonly known as Malware-as-a-Service (MaaS) who will typically develop different types of malware to later be sold to different threat actors such as cybercriminals or nation-state groups.

MaaS is one pillar in what is today refer to CaaS (Cybercrime-as-a-Service). It is an industry which has grown exponentially over the last years and is, today, one of the most prolific criminal activities supported by a consolidated and modern business model where vendors and clients can perform business transactions in trusted environment.

4.1. Cyber Threat Actors business model

As we have seen, the cyber threat actor ecosystem is large and complex. Typically, this is how the ransomware industry operates:

Selling Products & Services
Malware developers use "Dark Web" private and public forums, messaging applications or public websites to offer their products and services.

Attacking the targets
Threat actors, with the previously purchased tools, will attack their targets. They might also use previous stolen or purchased data, such as enterprise credentials to gain initial access.

Getting new sales channels
Other threat actors might use the purchased data as a new attack vector and can also request new developments to permform a new attack.

Monetizing the attack
Threat actors will get the ransom payment or set up an auction with the stolen data. If these fail they might publish the data for free to damage the organization's brand reputation.

5 How Cyber Threat Intelligence can help your organization

Intelligence can help organizations to reduce uncertainty and improve decision-making by understanding the threat landscape. Basically, it can help an organization to move from *Unknown Unknowns* to *Known knowns*.

An "*unknown unknown*" is a threat or risk that we do not know we do not know about, in other words, we are not aware that threat or risk even exists. On the other hand, a "Known Known" is something we know, and we understand.

With all these, we can also say that intelligence is: The process of moving from unknown unknowns to known knowns by discovering the existence of threats, understanding the risks, and mitigating them.

4.1. Cyber Threat Intelligence use cases

As we have seen, CTI can assist an organization by contributing to a more effective and efficient cyber risk management process.

There are several business use cases for an organization to leverage Cyber Threat Intelligence and these might vary according to the identified Intelligence gaps and the Priority Intelligence Requirements.

Here is how Cyber Threat Intelligence can help an organization considering the different intelligence subtypes.

STRATEGIC INTELLIGENCE

1. Help strategic decision-making processes by:

a. Understanding the threat and risk landscape.
b. Setting Priority Intelligence Requirements aligned with the business objectives.
c. Assisting to make the right decisions to address cyber-risks.
d. Helping to prioritize the organization's cyber security and IT budgets properly.

2. Communicate Cyber security Effectively by:

a. Advising senior management and the board on the different risks and threats the organization is exposed to and how these can be avoided or mitigated.

3. VIP & Executive Protection:

a. Preventing Spear-Phishing attacks to VIP and Executives by understanding who and why would target the organization's senior executives and board members.

OPERATIONAL INTELLIGENCE

1. Improve Incident Response Teams (CSIRT/CERT) capabilities by:

a. Improving incident triage.
b. Improving the Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR) to cyber attacks.
c. Providing context about specific attacks and who could be behind it.
d. Improving containment and remediation capabilities.

2. Contribute to Security Operations Center (SOC) teams by:

a. Improving prevention and detection capabilities.
b. Prioritizing and validating alerts.
c. Automating alert and event triage processes and thus enabling SOC analysts to stay focused on more relevant events.
d. Allowing Level 1 Analysts to make more precise decisions about alerts that should be escalated to the CSIRT/CERT.

3. Move from a reactive to a proactive security approach by:

a. Allocating more human resources and security personnel to relevant alerts rather than having them looking all day at thousands of logs and alarms.
b. Understanding the threat actor landscape and their motivations so the organize can act before a cyber-attack happens and prepare for it accordingly.

4. Promote Intelligence Sharing between colleagues or peer organizations.

TACTICAL & TECHNICAL

1. Assist in Vulnerability & Patch Management strategies by:

a. Identifying critical vulnerabilities that would likely be used by threat actors targeting the organization.
b. Tracking the weaponization and productization of exploits by different threat actors.
c. Helping Cyber Security Analyst with designing mitigation plans.
d. Communicating to the different stakeholders about the vulnerabilities that might not be mitigated immediately.

2. Contribute to Threat Hunting missions by:

a. Providing context about recent attacks, campaigns and threat actor attribution.
b. Contributing to Threat Hunting missions by understanding the TTPs used by different threat actors.

3. Incident Response Teams

a. Extracting and disseminating Indicators of Compromise of artifacts used in different attacks.

4. Network Defenders

a. Providing a technical IOC feed (IP Addresses, hash values, domains, urls, etc) to network defenders to blacklist these in network and end-point security technologies.

6 Choosing the right Cyber Threat Intelligence Vendor

Once we have understood key concepts about Intelligence Analysis and what is Cyber Threat Intelligence and how it can help our organization, we need to identify which are the intelligence needs or intelligence gaps. For this, it might be worth and useful to ask ourselves and the organization certain questions such as the following:

1. DOES THE ORGANIZATION HAVE A CYBER SECURITY STRATEGY?

2. IS THE ORGANIZATION MATURE ENOUGH, IN TERMS OF CYBER SECURITY, TO RUN ITS OWN CTI PROGRAM?

On the one hand, and as obvious as it may seem, if an organization does not have a proper cyber security strategy it will be difficult to implement a Cyber Threat Intelligence (CTI) program since this a discipline which has to be closely aligned with the organization's cyber security strategy.

It is normal that many organizations might not know about the threats they face, or which is their currently security posture and they will rather focus on buying security products based on industry trends or recommendations.

On the other hand, even if there is a cyber security strategy in place, an organization might not be cyber security mature enough to design, implement, and run its own CTI program. In this case, if the organization has identified it has an intelligence need it can contact the different CTI providers to address this need. Moreover, even organizations who run their own CTI program might want to contact these providers since they usually have analyst and resources that in-house teams might lack. What is more, working with these vendors can also be a way of helping in-house CTI teams to develop their own CTI skills.

3. CAN THE ORGANIZATION PREVENT, DETECT, AND RESPOND PROPERLY AND TIMELY TO INCIDENTS?

As we have seen, if the cyber security maturity level is not adequate and the organization does not have, for example, technologies that can provide system and network telemetry such as EDR (Endpoint Detection & Response) products it will be harder to detect incoming threats. In this case, the CTI team would not be able to get IoCs to enrich and provide context to the different security incidents. Therefore, in this case we can see that it would be important to have security products that could provide **technical intelligence** to be later enriched so that the CTI team can provide context to an incident.

4. WHICH ASPECTS DO WE WANT TO IMPROVE WITH REGARDS TO PREVENTION, DETECTION AND RESPONSE?

Prevention: this requires **strategic intelligence** that will allow and help decision-makers in designing a proper security strategy based in which industry the organization operates in, where is the company based and where are its main customers based. All this should help the organization to understand which is their threat landscape. This would also trigger the dissemination of tactical and technical intelligence to network security devices such as Firewalls or Proxies.

Detection: This requires operational intelligence to understand the nature of the attacks that might affect the organization and to learn from the threat actor's methodology and how we can detect it. For this matter, tactical and technical intelligence can be ingested to SIEMs to help improve the correlation rules. The same intelligence can be used to define detection rules in EDRs or even to define strategies for Threat Hunting teams.

Response: to improve the response capabilities all subtypes of intelligence are needed since the different intelligence products will help to enrich the IoCs and provide context about the incident and, hopefully, the threat actor along with his methodology and motivation behind it. This is important because it provides a framework related to the attack and will allow the organization to prepare a more efficient Incident Response plan in the post-incident phase as well as to improve the detection capabilities.

5. DOES THE ORGANIZATION HAVE THE NECESSARY TECHNOLOGIES AND HUMAN CAPABILITIES TO ACT UPON THE DIFFERENT INTELLIGENCE PRODUCTS?

To leverage the different intelligence products and services provided by a vendor, there might be a need to have certain technologies, if it is technical or tactical intelligence, and human capabilities if it is strategic or operational intelligence. The platform UX and UI might make a difference, especially for not skilled intelligence analysts or platform users and will therefore make a difference when assessing the vendor's intelligence products. A user who is not very skilled in Threat Intelligence, in some platforms, might find it difficult to understand where he should be looking for specific intelligence and how. Finally, we have to bear in mind that the intelligence products might need to be disseminated in multiple to different stakeholders. Therefore, the intelligence dissemination capability is important to understand if the intelligence products provided by the vendor will be easily ingested in other platforms such as Threat Intelligence Platforms (TIP) and Orchestrators.

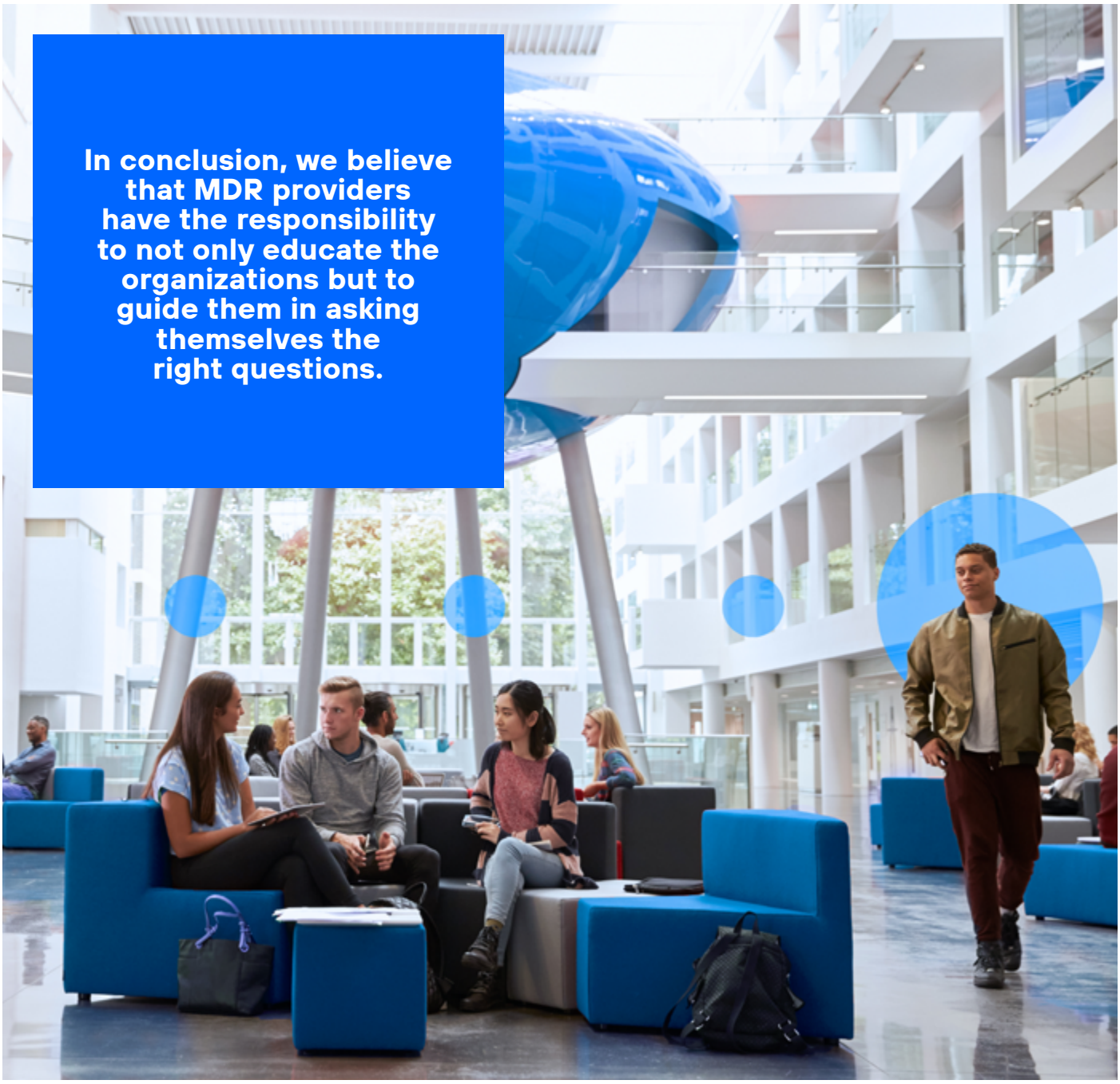
6. HOW DO WE PRIORITIZE IF THE SECURITY BUDGET CANNOT BE ADJUSTED TO THE INTELLIGENCE NEEDS?

To begin with, a CTI program should be aligned with the organization's cyber security strategy and it should help to address the different threats that the organization faces. There is not a unique Threat Intelligence vendor that excels at all capabilities and all intelligence subtypes. Therefore, if an organization does not have the necessary budget to run a CTI program there are options that can help the organization to start building the CTI capabilities, such as enriching IOCs with open-source platforms or ingesting open-source intelligence feeds to the different security tools. What is more, some Threat Intelligence providers offer technical intelligence feeds which, theoretically, have been curated and given context.

In an ideal scenario with no budget restraints, choosing every provider based only in its strengths would provide the best possible coverage.

As you can see, there is no secret sauce for choosing the right CTI provider. The key is to be able to ask the proper questions to understand how CTI products and services offered by any provider will help in reducing the identified intelligence gap or satisfying the identified intelligence needs.

In conclusion, we believe that MDR providers have the responsibility to not only educate the organizations but to guide them in asking themselves the right questions. For this matter, we believe that by mapping the answers to the different intelligence subtypes with the Threat Intel vendor knowledge we have; we are in a strong position to assist the organizations in finding a vendor whose services and products suits them best.



7 Cyber Threat Intelligence Maturity Model

To wrap-up and conclude this first article we would like to introduce a simple and concise maturity model to illustrate the way that organizations would use and leverage from a CTI program and CTI products and service according to their maturity.

NIST Cyber security Framework	-	Detect, Respond	Protect, Detect	Identify, Recover
Intelligence Type | Maturity	**Unaware**	**Reactive**	**Proactive**	**Predictive**
Strategic	No knowledge of the organization's threat landscape.	Senior managers are aware but may only act if peer organizations suffer a high impact cyber-attack.	Board members are aware. They receive and act properly upon intelligence.	Board members use intelligence to perform periodic Threat Modelling & Risk Assessments.
Operational	No planning to identify threat actors which might target the organization.	There is an Incident Response Team who will likely handle an incident.	CTI team tasked to investigate certain threat actors that would target the organization.	CTI team monitoring open and closed threat actor communication channels to provide the board with a clear situational awareness.
Tactical	No knowledge or awareness of how threat actors might target the organization (TTPs).	Knowledge of most common TTPs and attack vectors. Security Teams monitoring incidents in peer companies that could also affect the organization.	Intelligence Knowledge database maintained by the team to track threat actor activity and TTPs. CTI team providing the SecOps teams with actionable intelligence to protect the company.	Deep understanding of threat actor's TTPs and motivations. CTI team assisting.
Technical	No collection of relevant IOCs.	Extraction of IOCs after an Incident and dissemination to security devices.	Ingestion of public and private relevant IOC feeds to update blacklists.	IOC feeds are used by CTI teams to perform threat hunting missions to search for undetected malicious activity.

About Telefónica Tech

Telefónica Tech is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services and solutions in Cyber Security, Cloud, IoT, Big Data and Blockchain. Telefónica Tech's capabilities reach more than 300,000 customers in 175 countries every day.

More information

telefonicatech.com