Exploring the opportunities and limitations of current Threat Intelligence Platforms

PUBLIC

VERSION 1.0

DECEMBER 2017

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank all the subject-matter experts, from ENISA and external, who performed peer-reviews of the report, including:

1. Chris BEARD - CTI Expert, USA
2. Sarah BROWN - Security Links, The Netherlands
3. Alexandre DULAUNOY - Computer Incident Response Center Luxembourg (CIRCL), Luxembourg
4. Jane GINN - Cyber Threat Intelligence Network (CTIN), USA
5. Pasquale STIRPARO - CTI Expert, Switzerland

Table of Contents

1. Executive summary

As information security management is becoming a key component of any modern organisation, the need for relevant security data has seen a steady increase. But unlike traditional business data, in information security, relevance and context may originate from both within and from outside the organisation. It is for this reason, information sharing and the need for information sharing have become almost axiomatic in the world of cybersecurity. Topics such as information exchange formats and tools remain on the agenda of the cybersecurity community, in general, and of incident responders, in particular.

ENISA has been actively engaged in this dialog, by engaging communities interested in incident response taxonomies[1] or actionable threat information[2] (see [1] [2] [3] [4]). This paper should be viewed as part of an on-going fine-tuning process.

Our aim is to engage the topic of information sharing and analysis from a different angle, by focusing on some of the technical solutions proposed to share security relevant data within the community. We will collectively name these solutions Threat Intelligence Platforms (TIP).

Thus, the main objective of this report is to understand the limitations of threat information sharing and the analysis tools that are currently in use. Moreover, the second objective is to provide the relevant recommendations so that these limitations can be addressed and overcome. To achieve this, the report presents an overview of the users of these platforms, the main functional areas of TIPs as well as the current landscape of the TIPs used by different teams globally (CTI teams, SOCs, CSIRTs/CERTs, ISACs, etc.).

Finally, this report is meant to compliment the ENISA training material on incident and threat intelligence feed management[3], training material that focuses exclusively on the use of some of the TIPs mention in this report.

Among the main conclusion of this report, ENISA found that:

- **Organisation** should focus on their specific requirements and needs when developing and deploying TIP solutions;
- **Organisations** are highly recommended to log their requirements and work on how different cyber intelligence activities will be enabled by technology platforms;
- **Organisations** are encouraged to invest time on Proof of Concepts with an open source TIPs to familiarize themselves with the benefits of such systems, before making any significant financial investment;
- **TIP developers** and **vendors** are encouraged to focus on the enhancement of analysis capabilities of TIP that would help the end users on more efficient, threat triage and relevancy determination as well as threat analysis;
- **TIPs developers** and **vendors** should provide flexible and usable trust modelling functionalities for their solutions;

[1] ENISA A good practice guide of using taxonomies in incident prevention and detection, https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[2] ENISA paper on Actionable information for security incident response, https://www.enisa.europa.eu/publications/actionable-information-for-security
[3] ENISA trainings, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses

- **TIPs developers** and **vendors** are encouraged to provide consumers of threat information with functionalities which would allow them to be informed in case the confidence and accuracy of the shared information is not guaranteed by the source;
- The **research community** and **academia** should continue to pursue and investigate the benefits of TIPs and how these platforms may be further mature.

The main target audience of this report are: SOC analysts, Incident responders (and digital forensics), CTI analysts, Threat researchers and intelligence producers, Cyber fraud analysts and Vulnerability analysts.

Main contributions

This report provides:

1. Overview of main users of TIPs
2. Overview of existing TIPs
3. Identified limitations of TIPs and conclusions
4. Functional areas of TIPs
5. An indicative maturity model for TIPs

Methodology and information collection

A desk research was conducted based on publicly available information sources. ENISA deliverables have also taken into account, in particular [1], [2] and [3]. The focus was put on research papers, academic journals, publicly available information on threat intelligence and threat information sharing practices as well as whitepapers provided by the community. The intention is that the information provided, the findings and the recommendations should be vendor agnostic.

2. Threat Intelligence Platforms

TIP and Cyber Threat Intelligence

2.1.1 Current state of Cyber Threat Intelligence

During the past five years, the domain of cyber threat intelligence has emerged as a critical component of an organization's security operations capability. Cyber threat intelligence as a discipline has its roots in incident response and traditional intelligence [5] and there are various definitions, e.g. [6] [7] [8]. One illustrative definition of cyber threat intelligence is the below one:

> "*Cyber threat intelligence is the process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm*" [9].

According to the SANS CTI Survey 2017 [10], 60% of the responders already utilize threat intelligence for detection and response and 78% of them felt that it had improved their security and response capabilities. The table below presents some of the properties of threat intelligence, incident response and security operations practices [11]:

	THREAT INTELLIGENCE	INCIDENT RESPONSE	SECURITY OPERATIONS
Adoption	Early adoption phase	Mainstream since ~2010	Mainstream since ~2005
Focus	External threat monitoring	Security incidents and risk escalation	Notable security event monitoring
Best practices	Evolving best practices	Mature best practices	Mature best practices
Technology enablement	Limited technology enablement	Mature technology enablement	Mature technology enablement

Figure 1: Threat Intelligence, Incident Response and Security Operations practices [11]

Compared to incident response and security operations practices, threat intelligence is still in the early adoption phase. It is also a fact that best practices and maturity models for threat intelligence exist and are still evolving [12] [13] [10], while incident response and security operations have witnessed an improvement in terms of maturity.

Finally, a critical point is that technology enablement is limited in the threat intelligence practice, something that pinpoints the need for technology tools (especially of TIPs) that will help the analysts and their workflows towards efficient threat management. According to practitioners, lack of suitable technologies is one of the major factors (together with lack of staff expertise and ownership) determining why threat intelligence is not used effectively by organisations [14]. Moreover, organisations recognize that there is a need for tools that would help them manage the collected information and convert it to actions and knowledge [15].

2.1.2 What is a TIP?

An increasing number of organisations have started establishing or expanding their threat intelligence programs/practices. Threat intelligence programs implement processes that enable organisations to collect, analyse, produce and integrate their own and external intelligence. The utmost goal of any threat intelligence program is to produce intelligence that will be embedded into organisational workflows and would serve decision makers. The latter may also end up in driving operations to achieving policy outcomes.

Threat intelligence programs are comprised of people, processes and technology. A threat Intelligence Platform (TIP) is an emerging technology discipline that supports organisations' threat intelligence programs and helps them to improve their cyber threat intelligence capabilities. TIPs enable organisations to easily bootstrap the core processes of collecting, normalising, enriching, correlating, analysing, disseminating and sharing of threat related information. The TIP's critical role in threat management operations can be visually represented in the figure below [16]:

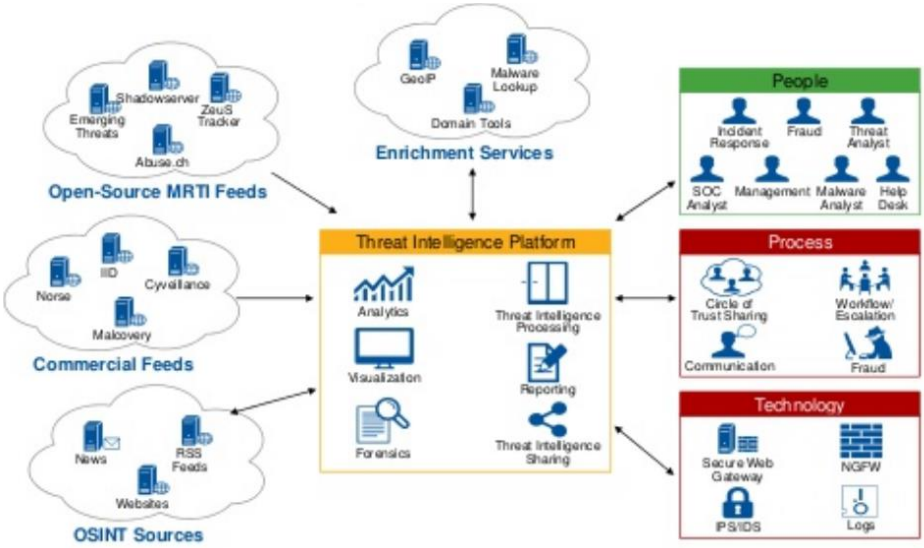

Figure 2: The ideal TIP [16]

2.1.3 Related work on TIPs

Despite the fact that TIP is quite a new technology toolset, there have been several publications and reports in this area. The most authoritative ones include the below: ENISA's report on "*Standards and tools for exchange and processing of actionable information*" [2], "*From Cyber Security Information Sharing to Threat Management*" [15], "*Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives*" [17], "*Towards improved cyber security information sharing*" [18], "*UX Aspects of Threat Information Sharing Platforms*" [19], "Technology Overview for Threat Intelligence Platforms" [20], "*Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice*" [21] and "*On the design of a cyber security data sharing system*" [22].

Current TIPs solutions

This section provides an overview of the TIP landscape where major TIPs are presented. The following table resumes different TIPs types:

Name	Type	Year	Owner	Project site(s)
Collaborative Research Into Threats (CRITs)	Open Source	2014	MITRE	https://crits.github.io/ https://github.com/crits
Collective Intelligence Framework (CIF)	Open Source	2012	CSIRT Gadgets Foundation	http://csirtgadgets.org/ https://github.com/csirtgadgets
GOSINT	Open Source	2017	Cisco	https://github.com/ciscocsirt/GOSINT https://gosint.readthedocs.io/en/latest/
MANTIS Cyber Threat Intelligence Management Framework	Open Source	2013	SIEMENS	https://django-mantis.readthedocs.io/en/latest/ https://github.com/siemens/django-mantis
Malware Information Sharing Platform (MISP)	Open Source / Community	2012	CIRCL	http://www.misp-project.org/ https://github.com/MISP https://www.misp-project.org/communities/
MineMeld	Open Source	2016	Palo Alto	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld https://github.com/PaloAltoNetworks/minemeld
Yeti	Open Source	2017	Yeti	https://yeti-platform.github.io/ https://github.com/yeti-platform
ThreatStream	Commercial	2013	Anomali	https://www.anomali.com/platform
EclecticIQ Platform	Commercial	2014	EclecticIQ	https://www.eclecticiq.com/platform
LookingGlass	Commercial	2015	LookingGlass	https://www.lookingglasscyber.com/products/manage-intelligence/
Soltra Edge	Commercial	2014	NC4	https://www.soltra.com/en/
Threat Central	Community	2015	Micro Focus	https://software.microfocus.com/en-us/software/cyber-threat-analysis
ThreatConnect	Commercial	2013	ThreatConnect	https://www.threatconnect.com/
ThreatQ Platform	Commercial	2015	ThreatQuotient	https://www.threatq.com/threatq/
TruSTAR	Commercial	2014	TruSTAR Technologies	https://trustar.co/
Open Threat Exchange (OTX)	Community	2012	AlienVault	https://www.alienvault.com/open-threat-exchange
ThreatExchange	Community	2015	Facebook	https://developers.facebook.com/products/threat-exchange
X-Force Exchange	Community	2015	IBM	https://exchange.xforce.ibmcloud.com/

2.1.4 Open source TIPs

- MITRE's Collaborative Research Into Threats (CRITs) [23] is an open source malware and threat repository that leverages other open source software to create a unified tool for analysts and security experts engaged in threat defence. CRITs employs a simple but very useful hierarchy to structure cyber threat information that gives analysts the power to 'pivot' on metadata to discover previously unknown related content.
- Collective Intelligence Framework (CIF) [24] is an open source cyber threat intelligence management system (most common types of threat information warehoused in CIF are IP addresses, domains and URLs). CIF enables combining known malicious threat information from many sources and using them for identification, detection and mitigation.
- GOSINT [25] is an open source framework used for collecting, processing, and exporting indicators of compromise. It is developed by Cisco CSIRT and can act as a powerful aggregator of indicators before they are passed to another analysis platform or to SIEM.
- MANTIS Cyber Threat Intelligence Management Framework [26] is an open source implementation of a framework for managing cyber threat intelligence expressed in standards such as STIX [27], CybOX [28], IODEF [29], etc. It is a threat information repository that also has browsing, filtering and searching capabilities.
- The MISP threat sharing platform [30] is a free and open source software solution for collecting, storing, distributing and sharing cyber security indicators and threat information about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals to support their day-to-day operations to share structured information efficiently. Finally, there are various MISP communities that an organisation can join [31].
- Palo Alto's MineMeld [32] is an open-source indicator processing framework. It has a modular architecture and it streamlines the aggregation, enforcement and sharing of threat indicators.
- Yeti [33] is an open source platform meant to organize observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository. Yeti will also automatically enrich observables and it provides an interface for humans and one for machines (via API) so that other tools can talk to it.

2.1.5 Commercial TIPs

- Anomali ThreatStream [34] is a commercial solution that allows organisations to collect, optimize, integrate and disseminate threat intelligence feeds. Indicators of Compromise (IOCs) are mapped with a strategic threat models so that analysts are able to quickly identify, investigate and react to security threats.
- EclecticIQ Platform [35] is a commercial Threat Intelligence Platform that delivers analyst-centric technology to consolidate, analyze, manage, action, and disseminate intelligence and reports. The platform is based on STIX and TAXII standards and provides analyst-friendly workflows as well as integration with top threat intelligence providers.
- LookingGlass [36] provides commercial solutions for managing intelligence and threats. ScoutPrime and ScoutVision provide the capability to collect, prioritize, and orchestrates the threat response as well as provide analysis, collaboration and threat sharing tools.
- NC4 Soltra Edge [37] is a commercial platform that automates processes to share, receive, validate and act on cyber threat intelligence. It uses STIX constructs to manage CTI which ensures easy interoperability with other applications and devices that are compliant with the STIX and TAXII standards.

- Micro Focus' Threat Central [38] is a community-sourced security intelligence sharing platform managed by HPE. The platform aggregates information from public feeds, security vendors, and community members which are analyzed and then subsequently disseminated to the relevant members of the community.
- ThreatConnect [39] is a commercial TIP solution that helps organizations to orchestrate security processes, analyze data, respond to threats, and report progress from a single location. It can also integrate with existing security tools and share intelligence with internal and external stakeholders.
- ThreatQuotient ThreatQ platform [40] is a commercial solution that focuses on cyber threat operations and management. It provides threat data aggregation capabilities, intelligence pivoting, customized workflows as well as orchestration and automation capabilities.
- TruSTAR threat intelligence exchange platform [41] is a commercial software-as-a-service solution. Main focus is put on operationalizing ISAC and OSINT feeds, streamlining internal processes and sharing as well as flexible information sharing with stakeholders.

2.1.6 Community Intelligence Exchange Platforms

- AlienVault Open Threat Exchange (OTX) [42] is an open threat intelligence community that enables collaborative defence with community-powered threat data. Organizations participating in OTX have the capability of automating the process of updating their security infrastructure with OTX's threat data.
- Facebook ThreatExchange [43] is a community-based Threat Intelligence platform managed by Facebook. Participating organizations can query, publicize and share threat data using a convenient, structured, and easy-to-use API that provides privacy controls to enable interacting with only desired groups within ThreatExchange.
- IBM X-Force Exchange [44] is a community-based and cloud-based threat intelligence sharing platform managed by IBM. Organizations using X-Force Exchange can research the latest global security threats, aggregate actionable intelligence integrate 3rd party intelligence feeds and collaborate with peers.

Users of TIPs

The following table summarises the main users of TIPs [45] [19].

Role	Major Contributions	Major Needs	Major Challenges
SOC analysts	1. SOC analysts provide feedback on indicators observed during triage phase. 2. They can also annotate indicators based on observations, alerts and actions taken.	1. Enhanced context and low false positive rates for basic indicators. 2. Vetted intelligence provided to SOC. 3. Automated data enrichment to reduce repetitive work. 4. Good integration with SIEM tools. 5. Playbooks and clear workflows. 6. Red flags related to key threats.	1.Too many alerts associated with threats, thus needing more context on which ones are the important ones and prioritize. 2. Lack of automation resulting in lots of manual tasks.
Incident responders (and digital forensics)	1. Incident responders can contribute new indicators and malware samples coming from investigations. 2. They can provide in depth analysis results from investigations and malware/log/forensics analysis. 3. Share tools and practices that helped them solve other problems.	1. Incident responders need tailored and ad-hoc intelligence related to tools, modus operandi, associated campaigns, actor intents and attributions, and forensic data for their investigations. 2. They also need detailed context and enrichment over the indicators provided. 3. Need to quickly identify if the investigated incident is part of a targeted attack and any other information that would help direct the response.	1. Lack of visibility into events across different systems or domains within the organisation. Thus, it is difficult to build the complete chain of the attack. 2. Manual tasks for collecting investigation logs/samples, for correlating collected data as well as for containing the incidents.
CTI analysts	1. CTI analysts are responsible for anything that goes in and out of the TIP (plus evaluate sources, intelligence and revise requirements). 2. They are responsible for enriching and analysing the data within TIP as well as linking intelligence. 3. Responsible for sharing intelligence with stakeholders (internal and external).	1. Need for a centralised platform for managing threat intelligence. 2. Unified relationship management with key internal and external stakeholders. 3. Trusted (personal and community) relationships for sensitive data sharing and trust in the access controls of the TIP. 4. Access and analysis from tactical to strategic threat intelligence.	1. Too much threat intelligence information floods CTI analysts who struggle to identify the most important and prioritise. 2. Too many manual tasks required for CTI analysts' workflows. 3. Lack of threat intelligence best practices and analysis capabilities toolsets.

Role	Major Contributions	Major Needs	Major Challenges
Threat researchers and intelligence producers	1. High quality original research conducted (potentially large amounts). 2. They have access to a number of sources and tools for their threat research and fusion. 3. They can conduct threat research, enrichment and analysis based on request and existing cases (RFI process).	1. Power users need APIs so that they can work on importing and exporting data from/to their toolset. 2. Ability to customize certain parts of TIP so that their workflows are supported (e.g. UI, more detailed indicators, etc.).	1. API support that is critical for the integration of power users' toolset. 2. Limited customization capabilities for TIP hinders the streamlining of their workflows.
Cyber fraud analysts	1. New indicators and samples related to cyber fraud. 2. Information on fraud related campaigns targeting the organisation.	1. Need to quickly identify if the investigated fraud is part of a complex attack and any other information that would help direct the response. 2. Expand their fraud investigation to identify other elements of the fraud. 3. Fraud attribution information.	1. Limited technology enablement to connect cyber and fraud datasets for investigation providing the relevant analysis tools.
Vulnerability analysts	1. Provide insight on the vulnerability exposure of the organisation.	1. Intelligence on high impact vulnerabilities of the organisations assets that can be exploitable. 2. Intelligence that would help them prioritise on patching and focusing on critical assets.	1. Prioritisation of the vulnerabilities to be patched.
Decision makers, IT Managers and Executives	1. They are the decision makers for sharing highly sensitive information. 2. They are responsible for the overall sharing policy and sharing culture for the organisation. 3. Decision makers for the security investment, staffing and budget related issues.	1. Decision makers need high level reports on exposures and the top threat that are relevant to the organisation in order to minimize risks. 2. Need to evaluate the ROI for intelligence investment via relevant investigation metrics. 3. Need to evaluate the ROI for external intelligence sharing via relevant metrics and evidence. 4. Assurance required that external intelligence sharing does not create risks for the organisation.	1. Decision makers have limited understanding of the organisation's exposures before a security incident takes place. 2. They are challenged to prove the value for intelligence investment.

3. Limitations

In this section, we present the limitations related to the current state and usage of Threat Intelligence Platforms. These limitations are not prioritised and are based on desk research, literature and feedback from practitioners.

Shared threat information is too voluminous

According to a recent survey [14], 70% of the responders replied that threat information shared is often too voluminous and/or complex to be actioned. One of the problems that this illustrates is the overload of threat information shared via open source, commercial sources as well as the private communities and ISACs. Combining shared threat information from different sources and industries makes the relevant intelligence hard to find and makes it difficult to generate value out of it [21].

Limited technology enablement in threat triage and relevancy determination

The aforementioned volumes of shared threat information combined with the limited threat triage and relevancy determination tools limit data accessibility [21]. There is limited technology enablement so that end users could efficiently facilitate the relevancy determination process [15].

Currently, this process is done manually, in a very complex way and it is dependent on the analyst. TIP capabilities that would help analysts are advanced searching, custom filtering, recommendation engines, (semi-)automated threat triage and building triage workflow [15]. Nevertheless, the above capabilities are not provided in many cases and the end users face the problem of managing and prioritizing the overwhelming threat information received ("distilling the signal from noise").

One would argue that while in previous years the major concern was providing incentives, standards and tools for information sharing, currently the problem has moved onto effective threat information management.

Sharing of the low hanging fruit

Research has identified that the majority of the platforms are focused on the tactical indicators of compromise [17]. There are cases that context is missing around the tactical indicators and this is something that hinders the work that needs to be done by CTI analysts and the recipients of the information.

During information sharing, standardized communication protocols are not commonly used and mostly unstructured PDFs or CSVs are exchanged [14]. On the other hand, whenever standards are used for threat information sharing then STIX 1.x, OpenIOC and MISP JSON are the most common ones. There has been observed an underutilisation of these standards when it comes to threat information sharing. For example, STIX 1.x is a quite expressive data model regarding cyber threat information and has some core constructs that comprise the STIX 1.x language. However, it has been observed that most of the tools share indicators of compromise that can be described by just two constructs of the STIX 1.x standard, Indicators and Observables. Thus, a current limitation is that that the low hanging fruit, tactical indicators of compromise, are mostly shared lacking comprehensive threat information while underutilising STIX 1.x data model. Some practitioners also argue that STIX is quite complex, that there is no common vocabulary for describing TTPs and that's why most of the intelligence producers focus on the Indicator and Observable constructs of STIX 1.x.

Data warehouses focusing on data collection

While technology is mostly focused on the collection phase of the intelligence, activities related to other phases of the intelligence cycle have been mostly neglected [17]. Only small fraction of activities mapped to the Processing and Exploitation, Analysis and Production as well as Dissemination phases could be adequately addressed by Threat

Intelligence platforms. Currently, Threat Intelligence platforms provide basic analysis capabilities which results in constraining analysts' capability to conduct comprehensive threat analysis, follow their intelligence workflows and usually be the bottleneck by doing lots of manual tasks. Taking into account the large amount of shared threat information and the limited analysis capabilities provided by TIPs, most of the current platforms end up being data warehouses rather than platforms where threat information can be shared and analysed.

Trust related issues

Researchers have identified trust issues related to the users and the platform providers [17]. Organisations participating in a Threat Intelligence platform (e.g. ISAC's platform), should have certain levels of trust towards the platform provider as well as the rest of the organisations and vice versa. The below trust relationships have been identified:

1. The organisation trusts the platform provider that the handling of the shared information and access controls does not expose confidential data to unauthorized recipients.
2. The organisation trusts the rest of the participant organisations that their handling of the shared information is done according to a predefined protocol e.g. TLP marking protocol [46], etc.
3. The platform provider (vendors, ISAC, etc.) and the rest of the organisations trust the organisation that the information shared by the organisation is reliable and credible.

TIPs, on the other hand, mostly provide access controls based on groups. TIP end users need more flexibility so that they can facilitate customizable, controlled and multilateral sharing among trusted peers.

The aforementioned trust relationships and limited TIP capabilities introduce several limitations in the way that organisations interact and contribute to specific communities. Organisations may select to share only specific types of threat data with specific communities and organisations moving closer to trusted and closed communities (or even peer to peer connections) to share highly sensitive data.

In addition, TIP developers and users should examine whether new legislation conditions are respected when such large data sets are being processed and used(for example, there are concerns in relation to GDPR).

Qualities of shared threat data and TIP limitations

Confidence is a property that is related to the quality of the shared information, something that is not provided by most of the feeds. Moreover, related work pinpointed that most of the shared STIX 1.x and APT reports provide incomplete information [47]. Context, quality data and confidence in shared data can help end users avoid undesired effects and not put additional effort on evaluating and verifying the received data [17].

Information provenance is all about assuring the quality of the shared data by tracking its evolution and is one of the hardest problems in information security [48]. Prior research has identified the TIP end users' need that provenance (and traceability) should be established [21].

Thus, there is a need to provide, track and handle confidence and provenance information (as metadata of the shared data) from different perspectives (consumer, producer and community) [15]. Existing data quality validation problems also stem from the inability to compare the different perspectives on the quality and confidence on the information shared.

Limited analysis capabilities

Practitioners use more email and spreadsheets compared to TIPs in order to aggregate, analyse and present CTI information [10]. This is indicative of the current limited intelligence analysis and management capabilities that are provided by TIPs, something that has also been identified by prior research [17]. More specifically, capabilities such as browsing, attribute based filtering, advanced searched information, pivoting, exploration and visualisation are some of

the major capabilities for which limitations have been observed [15]. Thus, the value of TIP is up to the analyst's tradecraft and ability to interpret, analyse, enrich and react to the threat information received.

Finally, only a small subset of the platforms provides integration with third party tools that could help addressing activities during the analysis phase of the intelligence cycle. Most common third-party tools that provide the pivoting and analysis capabilities are Paterva's Maltego [49], IBM's i2 Analyst's Notebook [50], Palantir [51], Tableau [52], Microsoft Excel [53], etc.

Diverse data models and formats used

Another limitation for TIPs is the variety of standards and data formats used to exchange threat information. While there are community efforts to provide connectors between different standards and formats [15], there are still limitations for TIPs that should collect, exploit and exchange of information between non-compatible standards and formats. Moreover, converting information without losing any elements or context from the initial/source format (lossless conversion) is also a challenge in threat intelligence (even a conversion between STIX 1.x and STIX 2.0 might lose information).

It is common practice that TIP owners are based on and support a specific framework and tend to stay with that framework. This is something that limits the flexibility of the TIP users in terms of the framework they work on and often results in a data model lock in.

Finally, it should be mentioned that the usage of different formats sometimes makes a lot of sense because they fit a specific need or purpose, e.g. Yara [54], Sigma [55], Suricata [56] rulesets, etc.

Limited advanced analytics capabilities and tasks automation

According to prior research, TIPs have currently limited advanced analytics capabilities [15], something that practitioners also verify [10]. These capabilities are related to the processing and exploitation phase of the intelligence cycle when new data are ingested and need to be analysed, enriched and linked with the existing ones.

Advanced analytics are vital for the subsequent analysis of the data, threat triage and relevancy determination, visualisation and pivoting. A TIP that has advanced analytics capabilities can generate complex relations between data such as aggregation, composition, generalization as well as the capability to de-duplicate, automatically tag and classify data. Since most of the shared threat data is tactical, routine tasks can be derived from advanced analytics be and automated. Some TIPs have introduced playbook/orchestration capabilities that can take further advantage of advanced analytics and help CTI analysts in their daily operations.

Time-to-live for shared intelligence is missing

Time-to-live information (expiration) of tactical threat indicators is very dependent on the end users of the TIPs along on the operative process of the organisation using the information [57]. It is critical, though, for the intelligence information since it can be used by the intelligence consumers to prioritize and act during the time window provided [15]. Moreover, the consumer could easily identify short-lived intelligence and could avoid taking action based on stale intelligence. Currently, the time-to-live information is not provided by most of the feeds and TIPs have limited capabilities in handling this type of metadata information. This is also verified by the practitioners that are not satisfied with the identification and removal of expired indicators of compromise [10].

Wide variety of APIs, data formats and requirements for integration

TIPs, as the centralised place where most of the activities of the intelligence cycle take place, should provide interfaces to the relevant third-party tools and services that are used by end users in the organisation. These

integration interfaces can be included in activities related to most of the phases of the intelligence cycle (from collection to dissemination).

Related to enterprise integration and API usage, some TIPs are more mature than others. However, the need for integration has extra challenges for TIPs that need to integrate with an ever-growing set of services and tools (security controls and workflow systems) with diverse APIs and requirements [15]. As a result, TIPs integrate with a (more or less) standard set of services and tools while requests for additional integrations are prioritized by TIP vendors as well as open source developers.

Limited workflow enablement

Currently, TIPs provide limited workflow capabilities that would make the process of threat management more efficient. Some specific examples include the capability of stakeholders to send RFIs (Requests for Information) to the analysts via the TIP, collaboration tools during analysis and production phase with a wider set of SMEs and capability to import iterative feedback loops on the intelligence product with the intended stakeholder. What is though encouraging is that some TIP vendors add collaboration functionalities ("Tasking" for broader teams) with some limited alerting on Task deadlines as well as chatting capability.

Threat knowledge management limitations

TIPs are also used as a threat knowledge management solution. Information about TTPs, threat actors and campaigns is managed and analysts use this knowledge base to track the activity of the relevant threats, actors and tools. Nevertheless, limitations have been identified in the way that this information is recorded within these platforms.

No common vocabulary is used for describing threat actors, TTPs as well as tools. A lot of freetext is provided even within STIX 1.x documents something that makes a structured analysis not relevant. Moreover, TIPs provide limited flexibility to use the vocabulary of other frameworks when needed e.g. MITRE'S ATT&CK framework [58].

4. Conclusions

In this section, we present some conclusions related to Threat Intelligence platforms and their usage from Threat Management teams. These recommendations are not prioritised and are based mostly on desk research, literature and feedback from the practitioners.

Organisations

4.1.1 Focus on requirements

CTI best practices include 3 lists of requirements that would help organisations evolve and mature their cyber intelligence programs. A lot of related work in this area gave insights on: collection requirements [59], defining requirements [60], setting requirements [61] how they fit into the intelligence cycle [62], defining collection priorities [63], how to collect requirements [12] and use them to drive a threat intelligence program [64]. The 3 lists of requirements are the following ones [65]:

- Production requirements that include the finalised product that will be delivered to the intelligence consumers and the stakeholders
- Intelligence requirements include what is needed to be collected to meet production requirements.
- Collection requirements include all the relevant data inputs to satisfy the intelligence requirements.

Maintaining and acting on these lists of requirements would help organisations prioritise resources, threat sources/data inputs and technology enablement needed to deliver their finalised intelligence products to the stakeholders. The requirements are very relevant to the role and the desired capabilities of the TIP so that it could play its central role in the threat management process.

4.1.2 Technology enablement via a TIP solution

Technology enablement is critical to manage the threat information shared via the different threat sources. Threat Intelligence Platforms are the means for collecting and managing this information as well as converting it into knowledge and actions [15]. This is in accordance with one of the service findings [14]: most organisations already use such platforms or plan to have one in the future and responders believe that handling and prioritizing this information would have been much more difficult without such platforms.

Organisations are highly recommended to log their requirements and work on how different cyber intelligence activities will be enabled by technology platforms. The utmost goal is that the TIP is not used as an indicator repository but as a tool that help them manage the cyber threats they face. TIP should fit the needs, requirements and use cases previously set and play a significant role, as a technology enablement, for the activities of the CTI team as well as the successfulness of the cyber intelligence program.

Finally, organisations are highly recommended to invest time on PoCs with an open source TIPs (e.g. MISP) to familiarize before making any significant financial investment.

4.1.3 Clear processes and policies on information sharing

Organisations should have clear processes and policies on what and how they facilitate information sharing [45]. A TIP solution can act as enabler for effective information sharing but is not enough by itself (no silver bullet) unless proper process, polices, sharing goals and objectives are established and clearly defined.

4.1.4 Using a standard data model for threat information

When it comes to threat information management and sharing, organisations should select the standard that fits theirs as well as their stakeholders' needs. The selected data model should not depend on free-text fields and there should be a common vocabulary [21]. The selected data model should be flexible enough to be adapted to stakeholders needs if needed.

TIP Users

4.1.5 Feedback to TIP owners/developers

The domain of TIPs is quite new just like Cyber intelligence practice. During the past years, TIPs have gone through massive development trying to cover the requirements of the TIP users that have different practices and approaches for their daily activities. Thus, feedback related to the technology enablement is critical so that TIPs can be further developed and satisfy the ever-growing list of requirements of the TIP users.

TIP users are highly recommended to work together with TIP owners so that a win-win situation can be achieved: TIP users can effectively use TIPs for their daily activities (and get ROI as well) and TIP owners can further develop the platforms and satisfy the requirements of TIP users. This can happen via Product Enhancement Requests for the commercial TIPs and via issue creation and active contribution in GitHub [66] for the open source TIPs.

The MISP example is indicative of how feedback and active contribution has enhanced MISP capabilities throughout the last years. There have been 2500 issues created in MISP GitHub page [67] from 12 April 2013 until 24 September 2017. The aforementioned feedback has played a significant role in MISP development, planning and adoption.

TIP Developers/Vendors

4.1.6 Analysis capabilities and TIPs

One interesting result of the SANS CTI Survey 2017 was that practitioners use more email and spreadsheets rather than TIP capabilities for aggregating and analysing threat information [10]. This is indicative of the limited analysis capabilities of TIPs and it is a fact that lot of analysis requires manual effort with "old school" tools.

Currently, TIPs are shifting towards providing threat intelligence management capabilities. Some of the TIPs already provide visualisation, advanced searching and workflow capabilities. Finally, there is also a need for TIPs to include standard APIs that would enable easy integration with other threat analysis tools of choice [15].

TIP owners should focus on the enhancement of analysis capabilities of TIP that would help the end users on more efficient, threat triage and relevancy determination as well as threat analysis.

4.1.7 Trust modelling functionalities

TIPs should focus on providing trust modelling functionalities [17]. Organisations should be enabled to form custom trusted and closed communities, direct connections and be able to provide anonymised data. TIPs should also give to the organisations the capability to control the security of the shared data (what information is shared, how much of it and with whom). These capabilities would act as a trust bond between the TIP and the organisations, that the TIP could actually be trusted and as a means of delivering, storing and managing sensitive threat data.

Finally, TIPs should finally enforce sharing back policies and verify what information is shared back to a community [15]. The latter would be something that will play a significant role in the trust building of the various information sharing communities.

4.1.8 Usage of APIs, integration and workflow enablement

Organisations and mostly TIP owners should focus on the widespread usage of APIs that would help towards enhanced automation, less manual activities and more integration opportunities. However, the integration of TIPs with security technologies and tools is still a big challenge according to practitioners [14].

Use of APIs should happen during almost every phase of the intelligence cycle. More specifically, extensive use of APIs is critical so that automated workflows could be built, manual tasks could be reduced, TIP users could have more time to focus on important tasks and be presented with enriched data with more context. For example, a good approach would be to minimize manual data fusion operations especially the ones related to publicly available sources e.g. DNS-lookups, WHOIS lookups [21].

Finally, focus should be also put on the workflow capability that can be enabled via the extensive usage of APIs. Integration with organisational workflows as well as streamlined workflow for threat analysis and intelligence production are capabilities that should be delivered via TIP in the next years. TIP should be the single pane of glass where the whole threat analysis will be conducted and task/activities will be followed up ("ditching the need for email discussions on threats and activities").

4.1.9 Threat data quality enhancement

TIPs should provide the capability to automate data quality error detection and establish common entry data rules [21]. Thus, shared data will go through a (customizable) quality control process [18].

Moreover, TIPs (as a trusted party) should have the capability to provide contextual information to the recipients of the shared information that is related to information provenance, quality and accuracy. Finally, consumers of threat information should be informed in case the confidence and accuracy of the shared information is not guaranteed by the source [12].

4.1.10 Flexible threat data management

TIPs should provide the capability to the end users to use the vocabulary and framework that fits their purpose. TIP owners usually stick to one standard/framework so the end users of the TIP are locked in the framework / standard that TIP owner uses. Towards the right direction is MISP Galaxy [68] as well as the data model of STIX 2.x that is really built for extensibility. TIP owners are recommended to follow the "Galaxy" approach and take full advantage of the STIX 2.x extensibility capabilities.

Intelligence Producers

4.1.11 Enhancing the quality of shared information

TIP users should provide confidence and accuracy metadata information related to the data they share [21]. It would be also preferable that redundant (automated and manual) error checking should be conducted at source. Moreover, the source of intelligence should also provide time-to-live indication of the shared data [15]. This is something that would help the consumers prioritize and better manage the received information.

4.1.12 Coherent use of the standards

The majority of current threat information exchange does not include standardized protocols. This mostly happens because current standard proposals have failed and the community prefer not to use any of those but to adapt to other formats. Despite the adoption of some standardized protocols, their standard vocabulary is underutilised e.g. STIX v1 Observable and Indicator constructs are used much more frequently than the other ones [17].

Intelligence producers should avoid using freetext in the shared information but rather put the information in the relevant "buckets" of the standard so that fusion analysis would be more effective by the intelligence consumers.

Intelligence producers are highly advised to take full advantage of vocabulary used in standards and use the wide variety of constructs that would provide more context to the information shared. Finally, the extensibility of STIX 2.x will provide even more opportunities for the STIX users to express the threats in a customisable and desired way.

CTI community and Researchers

4.1.13 Further research on TIPs

More research and evaluation studies are required in the field of TIPs since this new domain is still being explored.

More specifically, three interesting topics for future research are the following:

- Scientific research and evaluation of TIP user interface, analysis options, visualisation options and required functionalities [17].
- Empirical research on the value that TIP bring to the organisation and how data quality impacts this value [21].
- Provide a standardised definition of TIPs as well as define and research on the functional areas and capabilities of threat intelligence sharing platforms.

4.1.14 Further research on standards

CTI community members, researchers and OASIS CTI-TC [69] members could conduct research on some of the below topics:

- Researching on understanding the underutilisation of STIX 1.x.
- Work on resolving STIX 1.x complexities and providing additional capabilities for STIX 2.x (e.g. built-in extensibility, etc.).
- Investigate how STIX 2.x includes metadata like accuracy, provenance and time-to-live information and how can these practically be used via TIPs.
- Provide the relevant tools, connectors and guidance so that organisations can adopt STIX 2.x.
- Further research in lossless conversion between different formats/standards used in threat intelligence. Converting information without losing any element or context between different formats is still a challenge.
- Further research on Unified Cyber Ontology [70]. The Unified Cybersecurity Ontology (UCO) is intended to support information integration and cyber situational awareness in cybersecurity systems.
- Further research on MISP Active Internet Drafts [71]. Currently, there are 4 MISP Active Internet Drafts for MISP core format, MISP galaxy format, MISP object template format and MISP taxonomy format.
- Further research on OpenDXL [72]. OpenDXL is an initiative to create adaptive systems of interconnected services that communicate and share information for real-time, accurate security decisions and actions.
- Further research on Sigma which is a generic signature format for SIEM systems [55].
- Further research on IODEF [73].

5. Bibliography

[1] ENISA, “Information sharing and common taxonomies between CSIRTs and Law Enforcement,” 2015. [Online]. Available: https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement. [Accessed 07 July 2017].

[2] ENISA, “Standards and tools for exchange and processing of actionable information,” 2015. [Online]. Available: https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information. [Accessed 01 September 2017].

[3] ENISA, “Actionable Information for Security Incident Response,” 2014. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/new-guide-by-enisa-actionable-information-for-security-incident-response. [Accessed 01 September 2017].

[4] ENISA, “Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement,” 2017. [Online].

[5] CIA, “A Definition of Intelligence,” 1995. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm. [Accessed 01 September 2017].

[6] M. Cloppert, “Defining Cyber Threat Intelligence,” 2016. [Online]. Available: https://ctianalys.is/2016/08/22/defining-cyber-threat-intelligence/. [Accessed 01 September 2017].

[7] S. Caltagirone, “Threat Intelligence Definition: What is Old is New Again,” 2016. [Online]. Available: http://www.activeresponse.org/threat-intelligence-definition-old-new/. [Accessed 01 September 2017].

[8] Gartner, “Definition: Threat Intelligence,” 2013. [Online]. Available: https://www.gartner.com/doc/2487216/definition-threat-intelligence. [Accessed 01 September 2017].

[9] R. M. Lee, “Intelligence Defined and its Impact on Cyber Threat Intelligence,” 2016. [Online]. Available: http://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/. [Accessed 01 September 2017].

[10] SANS, “SANS 2017 CTI Survey,” 2017. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677 . [Accessed 01 September 2017].

[11] EclecticIQ, “A Stakeholder-Centric Approach to Building a Cyber Threat Intelligence (CTI) practice,” 2017. [Online]. Available: https://www.eclecticiq.com/downloads/EclecticIQ-White-Paper-A-Stakeholder-Centric-Approach-to-Building-a-Cyber-Threat-Intelligence-Practice.pdf. [Accessed 01 September 2017].

[12] NCSC, “Threat Intelligence: Collecting, Analysing, Evaluating,” 2015. [Online]. Available: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf. [Accessed 01 September 2017].

[13] Recorded Future, “Best Practices for Applying Threat Intelligence,” 2017. [Online]. Available: https://go.recordedfuture.com/applying-threat-intelligence. [Accessed 01 September 2017].

[14] Ponemon Institute, “The Value of Threat Intelligence: A Study of North American and United Kingdom Companies,” 2016. [Online]. Available: https://anomali.cdn.rackfoundry.net/files/white-papers/Ponemon-Research-Report.pdf. [Accessed 01 September 2017].

[15] S. Brown, J. Gommers and O. Serrano, “From Cyber Security Information Sharing to Threat Management,” in *WISCS '15 Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 2015.

[16] Gartner, “ Gartner Essentials: Top CybersecurityTrends for 2016-2017,” 2016. [Online]. Available: https://www.slideshare.net/SBAResearch/gartner-essentials-top-cybersecuritytrends-for-20162017. [Accessed 01 September 2017].

[17] C. Sauerwein, C. Sillaber, A. Mussmann and R. Breu, “Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives,” 2017.

[18] L. Dandurand and O. Serrano, “Towards Improved Cyber Security Information Sharing,” in *2013 5th International Conference on Cyber Conflict*, 2013.

[19] T. Sander and J. Hailpern, “UX Aspects of Threat Information Sharing Platforms,” 2016.

[20] Gartner, “Technology Overview for Threat Intelligence Platforms,” 2014. [Online]. Available: https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms. [Accessed 01 September 2017].

[21] C. Sillaber, C. Sauerwein, A. Mussmann and R. Breu, “ Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice,” in *WISCS '16 Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 2016.

[22] O. Serrano, L. Dandurand and S. Brown, “On the design of a cyber security data sharing system,” in *WISCS '14 Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 2014.

[23] MITRE, “MITRE's Collaborative Research Into Threats (CRITs),” 2014. [Online]. Available: https://crits.github.io/. [Accessed 01 September 2017].

[24] CIF, “Collective Intelligence Framework (CIF),” 2012. [Online]. Available: http://csirtgadgets.org/. [Accessed 01 September 2017].

[25] Cisco, “GOSINT,” 2017. [Online]. Available: https://github.com/ciscocsirt/GOSINT. [Accessed 01 September 2017].

[26] MANTIS, “MANTIS Cyber Threat Intelligence Management Framework,” 2013. [Online]. Available: https://django-mantis.readthedocs.io/en/latest/. [Accessed 01 September 2017].

[27] STIX, “Structured Threat Information Expression,” 2017. [Online]. Available: https://stixproject.github.io/. [Accessed 01 September 2017].

[28] CybOX, “Cyber Observable eXpression (CybOX),” 2017. [Online]. Available: https://cyboxproject.github.io/. [Accessed 01 September 2017].

[29] IETF, “An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information,” 2014. [Online]. Available: https://tools.ietf.org/html/rfc7203. [Accessed 01 September 2017].

[30] MISP, “MISP - Malware Information Sharing Platform,” 2012. [Online]. Available: http://www.misp-project.org. [Accessed 01 September 2017].

[31] MISP, “MISP Communities,” 2016. [Online]. Available: https://www.misp-project.org/communities/. [Accessed 01 September 2017].

[32] Palo Alto, “MineMeld,” 2016. [Online]. Available: https://github.com/PaloAltoNetworks/minemeld. [Accessed 01 September 2017].

[33] Yeti, “Yeti Platform,” 2017. [Online]. Available: https://yeti-platform.github.io/. [Accessed 01 September 2017].

[34] Anomali, “Anomali ThreatStream,” 2017. [Online]. Available: https://www.anomali.com/. [Accessed 01 September 2017].

[35] EclecticIQ, “EclecticIQ Platform,” 2014. [Online]. Available: https://www.eclecticiq.com/platform. [Accessed 01 September 2017].

[36] LookingGlass, “LookingGlass Manage Intelligence,” 2015. [Online]. Available: https://www.lookingglasscyber.com/products/manage-intelligence/. [Accessed 01 September 2017].

[37] NC4, “NC4 Soltra Edge,” 2014. [Online]. Available: https://www.soltra.com/en/. [Accessed 01 September 2017].

[38] Micro Focus, “Micro Focus Threat Central,” 2015. [Online]. Available: https://software.microfocus.com/en-us/software/cyber-threat-analysis. [Accessed 01 October 2017].

[39] ThreatConnect, “ThreatConnect,” 2013. [Online]. Available: https://www.threatconnect.com/. [Accessed 01 September 2017].

[40] ThreatQuotient, “ThreatQuotient ThreatQ,” 2015. [Online]. Available: https://www.threatq.com/threatq/. [Accessed 01 September 2017].

[41] TruSTAR, “TruSTAR Technology,” 2014. [Online]. Available: https://trustar.co/. [Accessed 01 September 2017].

[42] AlienVault, “AlienVault Open Threat Exchange,” 2012. [Online]. Available: https://www.alienvault.com/open-threat-exchange. [Accessed 01 September 2017].

[43] Facebook, “Facebook Threat Exchange,” 2015. [Online]. Available: https://developers.facebook.com/products/threat-exchange. [Accessed 01 September 2017].

[44] IBM, “IBM X-Force Exchange,” 2015. [Online]. Available: https://exchange.xforce.ibmcloud.com/. [Accessed 01 September 2017].

[45] T. Sander and B. Hein, “Usability and Incentives for Threat Information Sharing Technology,” 2016.

[46] FIRST, “TRAFFIC LIGHT PROTOCOL (TLP),” 2016. [Online]. Available: https://www.first.org/tlp/. [Accessed 01 September 2017].

[47] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer and B.-T. Chu, “Data-driven analytics for cyber-threat intelligence and information sharing,” *Computers & Security Volume 67, June 2017,* 2017.

[48] INFOSEC Research Council, “Hard Problems List,” *Cyber Security and Information Assurance Interagency Working Group (CSIA IWG),* 2006.

[49] Paterva, “Paterva's Maltego,” 2017. [Online]. Available: https://www.paterva.com/web7/. [Accessed 01 September 2017].

[50] IBM, “IBM i2 Analyst Notebook,” 2017. [Online]. Available: https://www.ibm.com/us-en/marketplace/analysts-notebook. [Accessed 01 September 2017].

[51] Palantir, “Palantir,” 2017. [Online]. Available: https://www.palantir.com/. [Accessed Septemeber2017 01 2017].

[52] Tableau, “Tableau Software,” 2003. [Online]. [Accessed 01 September 2017].

[53] Microsoft Excel, “Microsoft Excel,” 2016. [Online]. Available: https://products.office.com/en-gb/excel. [Accessed 01 September 2017].

[54] YaraRules Project, “YaraRules Project,” 2013. [Online]. Available: http://yararules.com/. [Accessed 01 September 2017].

[55] sigma, “sigma - Generic Signature Format for SIEM Systems,” 2016. [Online]. Available: https://github.com/Neo23x0/sigma. [Accessed 01 September 2017].

[56] Suricata, “Suricata IDS,” 2009. [Online]. Available: https://suricata-ids.org/. [Accessed 01 Septemberq 2017].

[57] MISP, “Sighting the next level,” 2017. [Online]. Available: http://www.misp.software/2017/02/16/Sighting-The-Next-Level.html. [Accessed 01 September 2017].

[58] MITRE, “Adversarial Tactics, Techniques & Common Knowledge,” 2016. [Online]. Available: https://attack.mitre.org/wiki/Main_Page. [Accessed 01 September 2017].

[59] CIA, “A Fresh Look at Collection Requirements,” 1995. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol4no4/html/v04i4a03p_0001.htm. [Accessed 01 September 2017].

[60] SANS ISC, “Defining Threat Intelligence Requirements,” 2016. [Online]. Available: https://isc.sans.edu/forums/diary/Defining+Threat+Intelligence+Requirements/21519/. [Accessed 01 September 2017].

[61] S. J. Roberts, “CTI SquadGoals - Setting Requirements,” 2016. [Online]. Available: https://medium.com/@sroberts/cti-squadgoals-setting-requirements-41bcb63db918. [Accessed 01 September 2017].

[62] M. Arena, “Cyber threat intelligence requirements: What are they, what are they for and how do they fit in the intelligence cycle?,” 2016. [Online]. Available: https://www.linkedin.com/pulse/cyber-threat-intelligence-requirements-what-how-do-fit-mark-arena. [Accessed 2017 September 2017].

[63] S. J. Roberts, “Intelligence Collection Priorities,” 2016. [Online]. Available: https://medium.com/ctisc/intelligence-collection-priorities-10cd4c3e1b9d. [Accessed 01 September 2017].

[64] B. P. Kime, “Threat Intelligence: Planning and Direction,” 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/threat-intelligence-planning-direction-36857. [Accessed 01 September 2017].

[65] M. Arena, “Cyber Threat Intelligence: Building and maturing an intelligence program that supports the business, not just the SOC,” 2017. [Online]. Available: https://www.slideshare.net/MarkArena/cyber-threat-intelligence-building-and-maturing-an-intelligence-program-that-supports-the-business-not-just-the-soc. [Accessed 23 September 2017].

[66] GitHub, “GitHub,” 2008. [Online]. Available: https://github.com/. [Accessed 01 Setepmber 2017].

[67] MISP, “MISP GitHub page,” 2013. [Online]. Available: https://github.com/MISP/MISP. [Accessed 24 September 2017].

[68] MISP, “MISP Galaxy,” 2016. [Online]. Available: https://github.com/MISP/misp-galaxy. [Accessed 01 September 2017].

[69] OASIS, “OASIS Cyber Threat Intelligence (CTI) TC,” 2015. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti. [Accessed 01 September 2017].

[70] Unified Cyber Ontology, “Unified Cyber Ontology,” 2016. [Online]. Available: https://github.com/ucoProject/uco. [Accessed 01 September 2017].

[71] IETF, “MISP Active Internet Drafts,” 2016. [Online]. Available: https://datatracker.ietf.org/doc/search/?name=misp&sort=&rfcs=on&activedrafts=on&by=group&group=. [Accessed 01 September 2017].

[72] OpenDXL, “OpenDXL,” 2016. [Online]. Available: https://github.com/opendxl. [Accessed 01 September 2017].

[73] Managed Incident Lightweight Exchange , “IODEF,” 2012. [Online]. Available: https://tools.ietf.org/wg/mile/. [Accessed 01 September 2017].

[74] Department of Defense, “Joint Publication 2-0, Joint Intelligence,” 2013. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf. [Accessed September 01 2017].

[75] Intel471, “Threat intelligence program checklist,” 2016. [Online]. Available: https://intel471.com/threatintelprogramchecklist.pdf. [Accessed 01 September 2017].

[76] Intel471, “Cyber Threat Intelligence: Maturity and Metrics,” 2016. [Online]. Available: https://www.sans.org/summit-archives/file/summit-archive-1492183163.pdf. [Accessed 01 September 2017].

[77] Department of the Army, “Information Collection,” 2012. [Online]. Available: https://fas.org/irp/doddir/army/fm3-55.pdf. [Accessed 01 September 2017].

[78] OpenIOC, “OpenIOC,” 2013. [Online]. Available: http://www.openioc.org/. [Accessed 01 September 2017].

[79] E. W. Burger, M. D. Goodman, P. Kampanakis and K. A. Zhu, “Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies,” in *WISCS '14 Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 2014.

[80] TAXII, “Trusted Automated Exchange of Intelligence Information (TAXII),” 2017. [Online]. Available: https://oasis-open.github.io/cti-documentation/. [Accessed 01 September 2017].

[81] MISP, “MISP Taxonomies,” 2015. [Online]. Available: https://www.misp-project.org/taxonomies.html. [Accessed 01 September 2017].

[82] DomainTools, “DomainTools,” 2002. [Online]. Available: https://www.domaintools.com/. [Accessed 01 September 2017].

[83] RiskIQ, “PassiveTotal,” 2014. [Online]. Available: https://community.riskiq.com/. [Accessed 01 September 2017].

[84] Whois XML API, “Whois XML API,” 2011. [Online]. Available: https://www.whoisxmlapi.com/. [Accessed 01 September 2017].

[85] Farsight, “Farsight DNSDB,” 2013. [Online]. Available: https://www.farsightsecurity.com/solutions/dnsdb/. [Accessed 01 September 2017].

[86] CIRCL, “CIRCL - Passive DNS,” 2015. [Online]. Available: https://www.circl.lu/services/passive-dns/. [Accessed 01 September 2017].

[87] mnemonic, “mnemonic Passive DNS,” 2014. [Online]. [Accessed 01 September 2017].

[88] BFK, “BFK - Passive DNS replication,” 2008. [Online]. Available: http://www.bfk.de/bfk_dnslogger.html. [Accessed 01 September 2017].

[89] CIRCL, “CIRCL Passive SSL,” 2015. [Online]. Available: https://www.circl.lu/services/passive-ssl/. [Accessed 01 September 2017].

[90] VirusTotal, “VirusTotal Intelligence,” 2004. [Online]. Available: https://www.virustotal.com/#/intelligence-overview. [Accessed 01 September 2017].

[91] Cuckoo Sandbox, “Cuckoo Sandbox,” 2012. [Online]. Available: https://www.cuckoosandbox.org/. [Accessed 01 September 2017].

[92] Payload Security, “VXStream Sandbox,” 2016. [Online]. Available: https://www.vxstream-sandbox.com/. [Accessed 01 September 2017].

[93] MaxMind, “IP Geolocation,” 2002. [Online]. Available: https://www.maxmind.com/. [Accessed 01 September 2017].

[94] IPVoid, “IPVoid,” 2010. [Online]. Available: http://www.ipvoid.com/. [Accessed 01 September 2017].

[95] Spamhaus, “The SpamHaus Project,” 1998. [Online]. Available: https://www.spamhaus.org/. [Accessed 01 September 2017].

[96] CIRCL, “ AIL framework - Analysis Information Leak framework,” 2014. [Online]. Available: https://github.com/CIRCL/AIL-framework. [Accessed 01 September 2017].

[97] Hunchly, “ Hunchly Daily Hidden Services Report,” 2017. [Online]. Available: https://darkweb.hunch.ly/. [Accessed 01 September 2017].

[98] OnionScan, “OnionScan,” 2016. [Online]. Available: https://onionscan.org/. [Accessed 01 September 2017].

[99] Onion Investigator, “Onion Investigator,” 2017. [Online]. Available: https://oint.ctrlbox.com/. [Accessed 01 September 2017].

[100] Anomali, “Modern Honey Network,” 2014. [Online]. Available: https://github.com/threatstream/mhn. [Accessed 01 September 2017].

[101] Recorded Future, “Recorded Future,” 2009. [Online]. Available: https://www.recordedfuture.com/. [Accessed 01 September 2017].

[102] Shodan, “Shodan,” 2009. [Online]. Available: https://www.shodan.io/. [Accessed 01 September 2017].

[103] Censys, “Censys,” 2015. [Online]. Available: https://censys.io/. [Accessed 01 September 2017].

[104] vFeed, “vFeed,” 2015. [Online]. Available: https://vfeed.io/. [Accessed 01 September 2017].

[105] Cambridge Intelligence, “KeyLines,” 2012. [Online]. [Accessed 01 September 2017].

[106] EclecticIQ, “Applying the Threat Intelligence Maturity Model to your organization,” 2016. [Online]. Available: https://www.eclecticiq.com/resources/white-paper-threat-intelligence-maturity-model. [Accessed 01 September 2017].

[107] TNO, “Towards a mature cyber threat intelligence practice,” 2017. [Online]. Available: https://www.tno.nl/media/9419/innovating-in-cyber-security.pdf. [Accessed 01 September 2017].

[108] M. Arena, “Cyber threat intelligence: maturity and metrics,” 2016. [Online]. Available: https://www.slideshare.net/MarkArena/cyber-threat-intelligence-maturity-and-metrics. [Accessed 01 September 2017].

[109] FireEye, “Intelligence integration services,” 2016. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/ds-isight-intelligence-integration-services.pdf. [Accessed 01 September 2017].

[110] W. Zhao and G. White, “An Evolution Roadmap for Community Cyber Security Information Sharing Maturity Model,” 2017. [Online]. Available: http://aisel.aisnet.org/hicss-50/eg/cybersecurity_and_government/2/. [Accessed 01 September 2017].

[111] ThreatConnect, “Maturing a threat intelligence program,” 2016. [Online]. Available: https://www.threatconnect.com/maturing-threat-intelligence-program/. [Accessed 01 September 2017].

[112] ENISA, “ENISA Programming Document 2017-2019,” 2017. [Online]. Available: https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019.

[113] ELK, “The Open Source Elastic Stack,” 2017. [Online]. Available: https://www.elastic.co/products.

[114] TheHive, “TheHive Project,” 2017. [Online]. Available: https://thehive-project.org/.

[115] ENISA, “A good practice guide of using taxonomies in incident prevention and detection,” 2016. [Online]. Available: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection. [Accessed 2017].

[116] ENISA, “ENISA – CERT Inventory,” 2015. [Online]. Available: https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe. [Accessed 06 07 2017].

[117] ENISA, “Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches’,” 2015a. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing. [Accessed 06 July 2017].

[118] ENISA, “Report on Cyber Security Information Sharing in the Energy Sector,” 2016. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing. [Accessed 06 July 2017].

[119] European Parliament and Council, “Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,” 06 July 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. [Accessed 06 July 2017].

[120] ENISA, “A good practice guide of using taxonomies in incident prevention and detection,” 2016. [Online]. Available: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection. [Accessed 07 July 2017].

[121] ENISA, “Considerations on the Traffic Light Protocol,” 2017. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol.

[122] ENISA, “Ontology and taxonomies of resilience,” 2011. [Online]. Available: https://www.enisa.europa.eu/publications/ontology_taxonomies. [Accessed 01 September 2017].

[123] F. E. Hagan, Research Methods in Criminal Justice and Criminology, 1997.

[124] G. J. Bayens and C. Roberson, Criminal Justice Research Methods, 2011.

[125] ServiceNow, “ServiceNow Security Operations,” 2017. [Online]. Available: https://www.servicenow.com/products/security-operations.html. [Accessed 01 September 2017].

[126] Department of Defense, “Joint Publication 1-02,” 2010. [Online]. Available: https://fas.org/irp/doddir/dod/jp1_02.pdf. [Accessed 01 September 2017].

[127] M. Cloppert, “Levels of Threat Intelligence,” 2016. [Online]. Available: https://www.sans.org/summit-archives/file/summit-archive-1492183308.pdf. [Accessed 01 September 2017].

[128] IntellIgence and NatIonal SecurIty AllIance, “Operational levels of cyber intelligence,” 2013. [Online]. Available: https://www.insaonline.org/wp-content/uploads/2017/04/INSA_OperCyberIntelligence_WP.pdf. [Accessed 01 September 2017].

[129] M. J. C. R. M. A. Eric M. Hutchins, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Lockheed Martin, 2011.

[130] Accenture, “Accenture Cyber Intelligence Platform,” 2016. [Online]. Available: https://www.accenture.com/us-en/insight-accenture-cyber-intelligence-platform. [Accessed 01 September 2017].

[131] IntelMQ, “IntelMQ,” 2015. [Online]. Available: https://github.com/certtools/intelmq. [Accessed 01 September 2017].

[132] CAPEC, “CAPEC - Common Attack Pattern Enumeration and Classification,” 2014. [Online]. Available: https://capec.mitre.org/. [Accessed 01 September 2017].

6. Initial Bibliography/References

ENISA. (2017). *ENISA Programming Document 2017-2019.* Retrieved from https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019

//All the works cited in the text should be listed in full at the end of a publication – in a 'References' list, if it includes only works cited in the text, or in a 'Bibliography' if any other works have been consulted but not directly cited within the text.

References are cited in the text using the author's surname and year of publication, for example (Barrett, 1991), and the bibliography is preparedin alphabetical order. Where an author has two or more publications cited from the same year, they should be listed as a, b, and so on, for example (Barrett, 1991a).

The following order should be adopted:

(i) author's surname and initial(s) or first name followed by a comma;
(ii) title of the work in italics and, where appropriate, edition number;
(iii) publisher, place of publication, year of publication, relevant pages, etc.:

Annex A: Acronyms

ACRONYM	DESCRIPTION
API	Application Programming Interface
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSIRT	Computer Security and Incident Response Team
CTI	
DAE	Digital Agenda for Europe
DG	Directorate General
DG CONNECT	(European Commission) Directorate General for Communications Networks, Content & Technology
ENISA	European Union Agency for Network and Information Security
EU	European Union
SOC	Security Operations Centre
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic Light Protocol
TTP	Tactics, Techniques and Procedures
ROI	Return On Investment
RFI	Request For Information
IDS	Intrusion Detection System
ISAC	Information Sharing and Analysis Center
SIEM	Security Information and Event Management
EDR	Endpoint Detection and Response
NCSC	National Cyber Security Centre

Annex B: TIP functional areas and maturity model

TIP functional areas

Based on the literature [17], a need has been identified to investigate and define how threat intelligence sharing platforms can address different activities within the intelligence cycle model [74]. In this section, a set of properties enabled by TIPs is provided per intelligence cycle phase as Functional Areas (FA).

Figure 3: Intelligence cycle

6.1.1 Planning and direction

The planning and direction phase of the intelligence cycle is the first phase of the intelligence process and its main focus is the definition of the priority intelligence requirements [74].

Currently, Threat Intelligence platforms have limited involvement in this phase of the intelligence cycle. Nevertheless, TIP should act as a technology enablement so that users of TIP can perform the below activities [75]:

Requirements and gaps

- FA1.1 Collect and manage the identified requirements. Ideally, 3 requirements lists should be managed: production requirements, intelligence requirements and collection requirements as suggested in [76].
- FA1.2 Collect and manage the identified knowledge gaps that have been identified.

KPIs

- FA1.3 Provide and manage Key Performance Indicators (KPIs) for the intelligence program. The KPIs can be the quality and quantity if finalized intelligence products, specific KPIs per intelligence phase, etc.

RFIs

- FA1.4 Process and manage stakeholders' Requests for Information (RFI). Stakeholders with or without access to the TIP should be able to send a RFI to the TIP about a specific threat, so it can be processed by the team.

6.1.2 Collection

The collection phase of the intelligence cycle is related to the gathering of the raw data required to produce the finalized intelligence product [77].

The collection phase of the intelligence cycle and its activities could be streamlined by the use of a TIP. More specifically, the complete functionalities of the TIP that are related to this phase are the following ones:

Data Ingestion

- FA2.1 Capability to ingest threat data from different sources. What is challenging here is the wide variety of different sources: open source feeds, Information Sharing and Analysis Centres (ISACs), private communities, commercial intelligence providers, intelligence exchange platforms etc.
- FA2.2 Capability to ingest threat data in as many different data models and standards: STIX 1.x, STIX 2.x [27], OpenIOC [78], CybOX [28], IODEF [29], custom, etc. [79].
- FA2.3 Capability to ingest threat data via a variety of different transport mechanisms: TAXII [80], HTTPS, REST API, RSS, email, SFTP, shared folders (SMB), etc. TIP should also support the cases where the information will be pushed to the platform as well as when the information should be pulled by the TIP.
- FA2.4 Capability to import threat data in a variety of data formats (XML, JSON, YAML, CSV, TSV, PDF, DOCX, TXT). This also includes emails, PDFs, via freetext, via browser plugins, etc.
- FA2.5 Capability to collect tactical, operational and strategic intelligence [3].
- FA2.6 TIPs should be also able to collect structured, semi-structured and unstructured intelligence.
- FA2.7 Capability to collect threat data from local and internal sources (e.g. internal organisation sandbox).
- FA2.8 Capability for customizable polling of feed sources (customizable periodicity).

Storage

- FA2.9 Capability to store the collected data securely [18].
- FA2.10 Capability to store the collected data at scale [18].
- FA2.11 Capability to store collected data and apply retain based on policies.
- FA2.12 Capability to index collected data for faster searching functionality.
- FA2.13 Capability to store collected data and enforce privacy laws, regulations and other restrictions.

6.1.3 Processing and exploitation

The processing and exploitation phase follows the execution of the collection plan. During this intelligence cycle phase, the capabilities of the TIPs can be grouped in three super categories: data normalization, data enrichment and access control. Regarding data normalisation capabilities of the TIP, the below ones have been identified:

Normalisation and data models

- FA3.1 TIP should have the capability to normalise all stored data in a common format/standard/data model.
- FA3.2 Capability to manage many different standards / data models and provide compatibility and correlation functions among them.
- FA3.3 Capability to process and extract information from multiple special types of data: binaries, PCAP, emails, certificates, etc. Indicative capabilities could be the extraction of DNS and HTTP data from PCAPs, identification of similar binaries by fuzzy hashing, binaries unpacking, extraction of metadata from multiple file types, etc.
- FA3.4 TIP should also be supported by a flexible data model where complex objects can be expressed and linked together to express indicators, campaigns, threat actors, relationships, etc.

Marking, taxonomies and classification

- FA3.5 Capability to apply custom tagging/marking. This could happen in a manual or in an automated and predefined way.
- FA3.6 TIP should be capable of applying (custom) taxonomies to threat data on a predefined or manual way [81]. There should also be the capability that the taxonomies would remain local and not shared.
- FA3.7 TIP should be capable of providing automatic classification of information.
- FA3.8 Capability to apply marking, tagging and confidence at event, attribute, feed and source levels in a predefined way.

Access control

- FA3.9 TIP should have all the flexible access control mechanisms to ensure what it is presented and shared, how much of it and with whom. The aforementioned access control mechanisms are critical for the trust needed towards the platform operations.
- FA3.10 TIP should have the capability to manage marking information e.g. TLP.

Data enrichment

- FA3.11 TIP should be able to provide enrichment of data. Major enrichment sources are Whois, DNS, PassiveDNS, malware intelligence, sandbox, PassiveSSL. Thus, TIP should be able to conduct the aforementioned enrichment as a built-in capability or via integration with the enrichment services:
  - Whois – e.g. built-in whois lookup, DomainTools [82], PassiveTotal [83], Whois XML API [84], etc.
  - DNS – built-in DNS and reverse DNS lookup
  - PassiveDNS - DomainTools [82], PassiveTotal [83], Farsight [85], CIRCL [86], mnemonic [87], BFK [88], etc.
  - PassiveSSL - [83], [89], etc.
  - Malware Intelligence and repositories – [90], etc.
  - Sandbox – Cuckoo [91], VxStream, [92], etc.
  - Geolocation – MaxMind [93], etc.
  - Reputation services – IPVoid [94], Spamhaus [95], etc.
  - Public information leaks – AIL [96], etc.
  - Datasets about crawled information from the darknet – Hunchly [97], OnionScan [98], Onion Investigator [99], etc.
  - Repositories based on backscatter in case of distributed denial of service attacks and honeypot services – organisation's honeypots, Modern Honey Network [100], etc.
  - OSINT services – Recorded Future [101], Shodan [102], Censys [103], etc.
  - ASN information – built-in ASN information lookup, etc.
  - Vulnerability intelligence – vfeed [104], etc.
- FA3.12 TIP should be able to provide enrichment in an automated way and based on predefined requirements.
- FA3.13 Capability to easily expand the enrichment modules and authoring custom ones.

Complex data processing and exploitation

- FA3.14 TIP should be able to (automatically) link brand new data to already existing data via direct association bindings. The automatic correlation could also identify relationships between attributes and indicators from malware, attacks campaigns or analysis.
- FA3.15 Capability to match and link imported intelligence against custom rules and signatures (e.g. regular expressions, whitelists, blacklists, Yara rules, etc.) and apply

subsequent predefined actions (e.g. identify internal IP addresses and do not tag them as indicators).

- FA3.16 Taking into account the complexity of the cyber domain, TIP should be able to (automatically) link brand new data to already existing data via complex bindings such as aggregation, composition, generalization or realization [15].
- FA3.17 TIP should have the capability to de-duplicate threat information from various data sets.
- FA3.18 Capability of processing that supports data fusion, clustering and analytics.
- FA3.19 Capability to extract objects and entities from structured data based on common techniques.
- FA3.20 Capability to extract object and entities from unstructured data based on common and advanced techniques (Natural Language Processing, etc.).
- FA3.21 Capability to dynamically generate indicator signatures.
- FA3.22 Capability to generate warnings based on custom signatures and rules, before and after data enrichment.
- FA3.23 TIP should have the capability to determine provenance and confidence information from different perspectives [15].
- FA3.24 Capability to provide sightings support and process sightings information.

6.1.4 Analysis and production

This is the phase where the TIP users analyse all the information that was collected and enriched during the previous phases in order to produce intelligence.

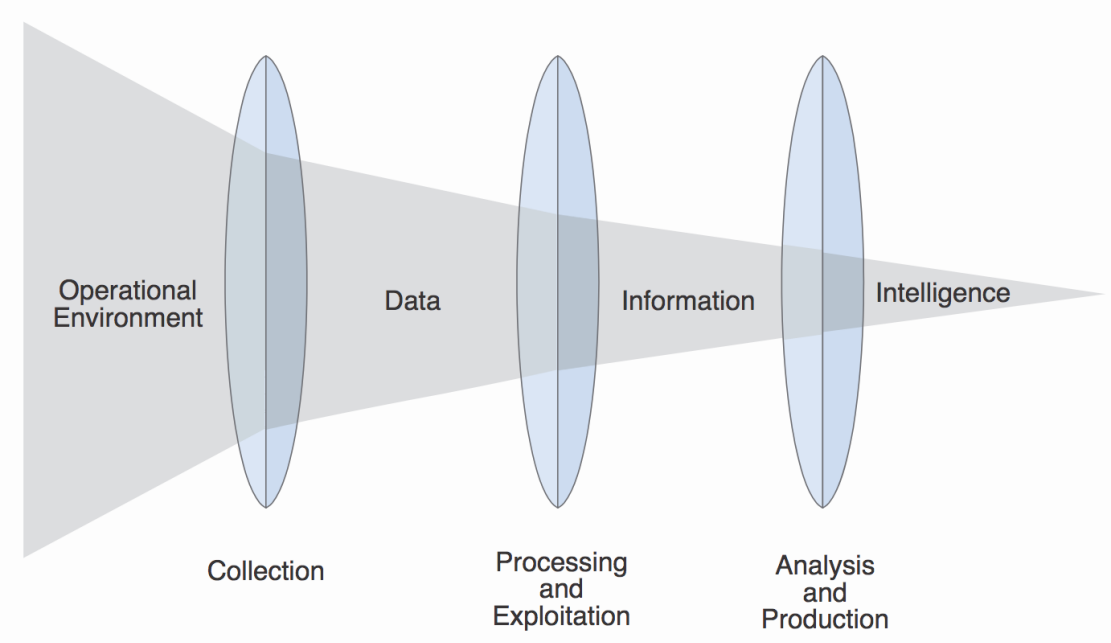

Figure 3: From data collection to intelligence analysis and production [74]

Regarding analysis and production capabilities of the TIP, the below ones have been identified:

User Interface and API

- FA4.1 TIP should provide a human interface for the analysts.
- FA4.2 TIP should support strong authentication (2 factor authentication) for the end users that that login via the user interface.
- FA4.3 Capability to provide enrichment on demand via a human interface.

- FA4.4 TIP should provide a machine interface and a detailed API. The API should be able to add and edit threat information as well as malware samples.
- FA4.5 Capability to provide RBAC so there is different UIs and information access per role.

Exporting capabilities

- FA4.6 TIP should provide the capability to export data manually in various formats (STIX, STIX2, OpenIOC, IDS signatures, Yara rule, XML, CSV, etc.) and based on different data attributes (indicator type, time, tag, keyword, etc..).
- FA4.7 TIP should provide the capability to export data via the API in various formats (STIX, STIX2, OpenIOC, IDS signatures, Yara rules, XML, CSV, etc.) and based on different data attributes (indicator type, time, tag, keyword, etc..).

Collaboration and workflow

- FA4.8 TIP should enable analysts building custom workflows.
- FA4.9 TIP should provide the capability for custom workflows that will enable multi-step approval for actions affecting sensitive data [18].
- FA4.10 TIP should provide chatting capability so that collaboration on threat triage and analysis can be more direct.
- FA4.11 TIP should provide the capability and tools to enable collaboration with internal and external stakeholders on threat triage, analysis and response. Iterative processes should also be able to be established so that each individual can provide his/her perspective and feedback [15].
- FA4.12 Stakeholder management capabilities.
- FA4.13 TIP should provide tasking capability, alerting on task deadline and logging analysts' activities (so that changes can be tracked).

Visualisation, pivoting and fusion

- FA4.14 TIP should provide a human interface that will be customizable for data visualisations (visual graph-based representation).
- FA4.15 TIP should provide the capability to visualise trend information over the data and other characteristics via data exploration.
- FA4.16 TIP should provide pivoting capabilities over data.
- FA4.17 TIP should provide that capability of integrating with 3rd party industry standard tools for data visualisation and link analysis like Paterva's Maltego [49], IBM's i2 Analyst's Notebook [50], Palantir [51], Tableau [52], KeyLines [105], etc.
- FA4.18 TIP should provide the capability to fusion structured, semi-structured and unstructured data from different sources, feeds and types.

Threat knowledge management

- FA4.19 Capability to relate tactical to strategic intelligence.
- FA4.20 TIP should provide the capability for the analysts to monitor operational intelligence and threat bulletins.
- FA4.21 TIP should provide the capability of building and managing a threat actor library and registering the relevant TTPs.
- FA4.22 TIP should provide the capability to register threat actors' attributes based on well-known standards e.g. STIX [27] as well as custom ones.
- FA4.23 TIP should provide the capability of using custom vocabularies e.g. for TTPs the MITRE's ATT&CK [58], for threat actors, custom vocabularies, etc.
- FA4.24 Threat actor management and tracking capabilities.
- FA4.25 Threat campaign management track capabilities.
- FA4.26 Threat incident management and tracking capabilities.
- FA4.27 Threat topic management and tracking capabilities.

- FA4.28 Capability to manually assign and tags and marking to threat information via the UI.
- FA4.29 Support well known intelligence and cyber intelligence frameworks e.g. kill chain, diamond model, TLP, NATO Admiralty code, estimative language, ATT&CK framework, etc.

Tactical intelligence management

- FA4.30 TIP should provide the capability of effective tactical indicator management with assurance that information is of relevant quality and fit for purpose.
- FA4.31 Capability to automate or semi-automated threat triage.
- FA4.32 TIP should enable analysts prioritize IoCs and threats by helping them determine intelligence relevance based on technical constructs and organizational input [15]. This could be achieved via rule-based or heuristics-based recommendation engines for threat information processing.
- FA4.33 TIP should provide the capability to the analysts to enrich the data with confidence scores, ratings, tags, prioritizations, annotations, etc.
- FA4.34 TIP should provide the capability for the analysts to easily maintain their watchlists (e.g. domain resolution watchlist) and provide alerting based on predefined criteria.
- FA4.35 TIP should provide the capability for the analysts to manage their rule signature base e.g. Yara rules [54] and receive alerts based on local data co-relation or external services integration e.g. VirusTotal Intelligence [90].

Search capabilities

- FA4.36 TIP should have a search capability that would enable analysts find and filter the relevant information based on content.
- FA4.37 TIP should have a powerful search capability that would analysts to find and filter the relevant information based on relationships, similarity and overlap with other intelligence items.
- FA4.38 TIP should have the functionality of privacy-preserving querying.
- FA4.39 Capability to search content with TIP via API usage.

Statistics, analytics and metrics

- FA4.40 TIP should use statistics methods and present them to the analysts so that trends can be identified and data analysis would be simplified.
- FA4.41 TIP should use advanced data analytics and present them to the analysts so that trends can be identified and data analysis could be simplified.
- FA4.42 TIP should be able to collect metrics on usage of threat data to enable ranking of feeds and sources.

Integration and automation

- FA4.43 TIP should integrate with SIEM, EDR solutions and security big data lakes so that search for high confidence IoCs can be automated and can act as an enabled for CTI analysis. These searches may try to identify IoC in real time or historically.
- FA4.44 Capability to integrate with workflow systems so that intelligence analysis tasks can be automated as much as possible.

6.1.5 Dissemination

The dissemination phase of the intelligence cycle follows the analysis and production phase. At this phase, intelligence has already been produced and is disseminated to the relevant internal and external stakeholders as well as to the organisation's security controls. The functionalities of the TIP that are related to this phase are the following ones:

Information sharing and dissemination

- FA5.1 TIP should provide the mechanisms for easy sharing of information to internal as well as external stakeholders based on specific criteria.
- FA5.2 TIP should have the capability to exchange threat data of different standards and models.
- FA5.3 TIP should be able to disseminate the information to the stakeholders in a predefined way satisfying the timing requirements e.g. real-time, frequency, time of day, etc.
- FA5.4 TIP should be able to disseminate the relevant data in the appropriate format that is agreed with stakeholder e.g. Microsoft Word, PDF, csv, STIX document, etc.
- FA5.5 TIP should have the capability of sending notifications and repots (e.g. via email) based on predefined criteria e.g. from specific sources, for specific threats, etc.
- FA5.6 TIP should support the standard transfer protocols for threat information exchange e.g. [80].
- FA5.7 TIP should have the capability to send the information to multiple systems and enable multilateral sharing.
- FA5.8 TIP should be able to use tagging for sharing information with specific peers, circles and communities.
- FA5.9 Capability to send the produced intelligence reports to the relevant stakeholder directly from the TIP.
- FA5.10 TIP should encrypt and/or signing the notification and information sent to stakeholders.
- FA5.11 Capability to disseminate indicators, threat reports, threat actor profile reports campaign reports and incident information reports.
- FA5.12 capability to disseminate alerts based on predefined criteria.
- FA5.13 TIP should have audit trail for intelligence that has been shared.

Privacy and trust

- FA5.14 TIP should be able to provide trust modelling functionalities e.g. forming closed communities, peer to peer connections.
- FA5.15 TIP should be able to apply policies via access control mechanisms on what is shared as well as what is disseminated, to whom and to what extent.
- FA5.16 TIP should be able to sanitize and anonymize information before being shared with the rest of the stakeholder where appropriate.
- FA5.17 TIP should provide the mechanisms for the organisation to identify sensitive data and replace them with privacy protected label before being shared [18].
- FA5.18 TIP should have the capability to allow organisation share intelligence data anonymously.
- FA5.19 Capability to provide granular access policies e.g. an intelligence product can have different parts that are TLP RED while the other parts may be TLP Amber.

Information sharing metadata

- FA5.20 TIP should have the capability to disseminate provenance and confidence information from different perspectives [15].

Sharing workflows

- FA5.21 TIP should provide the capability for custom workflows that will enable multi-step approval for actions affecting sensitive data, e.g. information sharing of sensitive data [18].

- FA5.22 TIP should incorporate collaboration, iteration, and feedback between threat intelligence analysts and the recipients of the intelligence after delivery. Thus, intelligence consumers can directly collaborate with the analyst, jointly revise of the intelligence product as well as inform on the required actions in response to a threat.

Integration and automation

- FA5.23 TIP should integrate with a large number of the security controls e.g. IDS, proxy, firewall, SIEM, EDR solutions and security big data lakes.
- FA5.24 TIP can have the capability to automate the proposed courses of action.
- FA5.25 TIP should have audit trail for intelligence integration.
- FA5.26 Capability to integrate with workflow systems so that intelligence is directly delivered into organizational workflows.

Metrics

- FA5.27 TIP should be able to report high level metrics useful for management level staff and that would help in overall risk management.

TIP maturity model

Based on the functional areas of the TIP provided in the previous section, we hereby provide a TIP maturity model. Thus, in this section we focus on the Technology part however Threat Management as a practice includes People and Processes as well. This is critical for the success of the Cyber Threat Intelligence program of an organisation since a common situation is organisation that have a mature TIP solution but are less mature with processes.

Relevant work regarding the Threat Intelligence Maturity Model has been conducted [12] [106] [107] [108] [109] [110] [111]. The threat intelligence program includes technology, processes and people, below the TIP maturity model is focused mostly on the technology part where TIPs play a central role:

- Level 1: Crawl
  - At this level, the organisation is mostly on tactical intelligence collection and consumption and very basic functionalities of a TIP platform are used. While consumption of a tactical feed is partially implemented (integration with security controls), there is no ability to analyse the intelligence and evaluate the threat sources. Sharing intelligence to the stakeholders is done in an ad-hoc way, based on personal contacts and not in a standard way (no sharing policy defined). Intelligence and intelligence products are somewhat integrated in the security controls.
- Level 2: Walk
  - At this level, the organisation starts actively taking advantage of TIP functionalities. TIP is used to import internal intelligence and deploy indicators per device (security control). TIP also is the central point where structured and unstructured intelligence from a wide range of sources: open source, commercial, ISACs, community, etc. is stored and enriched. TIP provides the proper assurance for access controls as well as secure storage and transport mechanisms. TIP has also the capability of providing basic insights on the intelligence managed as well as basic analysis functionalities. Intelligence products start being delivered consistent to stakeholders and standards are used when sharing externally.
- Level 3: Run
  - At this level, the organisation uses the TIP as a strategic tool of choice for threat triage, management and response. Stakeholders requirements are clear and threat sources are evaluated periodically via TIP provided capabilities. TIP provide awareness and insight on the processing that has already been done. TIP provides a range of threat analysis and fusion capabilities as well as analyst workflow building and collaboration functionalities. Dissemination is done in a systematic way to internal and

external stakeholders and integration into security controls and organisation workflow is fully implemented.

- Level 4: Fly
  - At this level, TIP is the single pane of glass for the analysts and the stakeholders. TIP provides capabilities during all the phases of the intelligence cycle, automation is extensively used and intelligence input is heavily embedded in the organisation. There are formal RFI, requirements, intelligence policies, iterative evaluations and intelligence products. TIP is powerful in threat management and analysis provided advanced awareness and analytics to the end users. Information sharing is strategically done via the TIP and the organisation uses the TIP as the major workflow and collaboration tool for the intelligence products.

	TIP MATURITY LEVEL 1	TIP MATURITY LEVEL 2	TIP MATURITY LEVEL 3	TIP MATURITY LEVEL 4
Direction and Planning				FA1.1, FA1.2, FA1.3, FA1.4
Collection	FA2.1, FA2.2, FA2.3, FA2.4, FA2.9	FA2.5, FA2.6, FA2.7, FA2.8, FA2.10, FA2.11, FA2.12, FA2.13		
Processing and exploitation	FA3.1	FA3.2, FA3.4, FA3.5, FA3.6, FA3.7, FA3.9, FA3.10, 3.111, 3.12, FA3.14, FA3.17, FA3.19, FA3.21	FA3.3, FA3.8, FA3.13, FA3.15, FA3.16, FA3.18, FA3.22, FA3.24	FA3.20, FA3.23
Analysis and production	FA4.1	FA4.2, FA4.3, FA4.4, FA4.5, FA4.6, FA4.7, FA4.14, FA4.19, FA4.20, FA4.21, FA4.22, FA4.28, FA4.30, FA4.31, FA4.33, FA4.34, FA4.36, FA4.39, FA4.40	FA4.8, FA4.10, FA4.11, FA4.12, FA4.15, FA4.16, FA4.17, FA4.18, FA4.23, FA4.24, FA4.25, FA4.26, FA4.27, FA4.29, FA4.32, FA4.37, FA4.38, FA4.41, FA4.43, FA4.44	FA4.9, FA4.13, FA4.35, FA4.42
Dissemination	FA5.1	FA5.2, FA5.3, FA5.4, FA5.5, FA5.6, FA5.7, FA5.12, FA5.15, FA5.23	FA5.8, FA5.9, FA5.10, FA5.11, FA5.13, FA5.14, FA5.16, FA5.17, FA5.18, FA5.24, FA5.25, FA5.27	FA5.19, FA5.20, FA5.21, FA5.22, FA5.26

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu