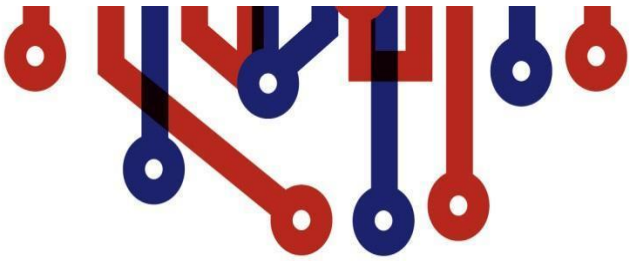


Threat Intelligence Management

An EE-ISAC White Paper

Table of Contents

List of Abbreviations

CRITs	Collaborative Research Into Threats
CTI	Cyber Threat Intelligence
CTM	Cyber Threat Management
DCS	Distributed Control System
ICS	Industrial Control System
IoC	Indicators of Compromise
IR	Incident Response
ISMS	Information Security Management System
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
TTP	Tactics, Techniques and Procedures

Foreword

The mission of the European Energy ISAC is to share knowledge among the network of trust in order to increase the resilience of the European Energy system: this acquires particular relevance in discussions about incident response in our community.

Many experts suggest that once security of infrastructure is compromised, especially in the electricity sector, it is already too late and the battle against the attacker is lost. At this point, from a security analyst´s point of view, the strategy should focus on shifting the priority entirely from event management to prevention and planning of countermeasures. From the perspective of an operator, however, response remains a big issue and entails the design, organization and nurture of a vast range of procedures.

Furthermore, this complex topic is beyond the scope of the most recent regulations and guidelines because, again, their provisions focus on risk analysis, risk mitigation and incident reporting.

EE-ISAC members were urgently required to meet for joint discussions about best practice, taking as our starting point the basics of standards and shared experiences; we soon discovered that the available material was too generic and that our research would become an opportunity.

We embarked upon a new journey with our contributors - including operators, vendors and academics - to create a living document in which we could address the problems and describe those solutions that we find feasible, scalable and sustainable for our organizations.

The following pages are the result of this journey. We are confident that further suggestions will emerge in the upcoming months and that new contributors could further enrich our community.

Thank you for your interest in EE-ISAC.

Introduction

EE-ISAC aims to help utilities improve their resilience to cyber-attacks by enabling information sharing and improving cyber security awareness across the energy sector. EE-ISAC has gathered together the combined experience of its membership to offer some useful guidance for adequate preparations for and response to cyber incidents, especially to assist smaller businesses. As a result, the EE-ISAC has published a white paper for “Cyber Security Incident Response” in the energy sector.

EE-ISAC members believe that Threat Intelligence can play a very important role in both preventive and reactive cyber security. Considering the additional complexity arising from Industrial Control System (ICS) Attack Vectors, the energy sector, even more than any other sector, seems to depend on good Threat Intelligence Management. This additional complexity arises, among other factors, from the following energy sector-specific characteristics:

- OT Networks – Utilities have to deal not only with attack vectors on Operational Technology (OT) and ICS but also on commodity IT/Enterprise Networks, as threat groups pivot through Enterprise Networks to gain access to ICS networks. Therefore, vulnerabilities and interconnections of Enterprise Networks and OT networks need to be understood.
- Remote Connections – The air-gap is a concept that is gradually disappearing because of the IT/OT convergence. Connections from the Enterprise Network to the OT Network are needed by field engineers and third parties carrying out maintenance tasks. Whether remote access can be abused depends on the technology used (Citrix/RDP), authentication, encryption and monitoring.
- Vendor Connections – Remote maintenance by third party vendors is vital to operations. Third parties and the threats on the supply chain need to be managed, ensuring that these third parties are operating with comparable maturity regarding cyber security.
- Privileged Users – Often in legacy components and Programmable Logic Controllers (PLC), only administrative access is possible. How is access achieved, and how can it be controlled?
- Employees – The primary responsibility of employees lies in operating the facility rather than in IT/OT security. Thus a lack of awareness regarding security topics can pose a big problem for utilities. An unaware employee in OT, for example, can allow an attack to bypass security controls, permitting an attacker access to the utilities’ most critical systems.
- Supply Chain – Hardware and Software vendors constitute potential threats that are hard to manage. Security Awareness by vendors is supported by legislation applicable to increasing numbers of vendors. What utilities can do is to keep detailed asset inventories and to manage them actively.
- Poorly Maintained Assets – The extended lifetime of Supervisory Control and Data Acquisition (SCADA) components and PLCs in particular results in a reduction in management capabilities and thus in assets whose maintenance is less than optimal.

Usually, these challenges would be addressed by an Information Security Management System (ISMS), which collects relevant logs and information. However, any system is only as good as the information provided to it. For utilities in particular, Threat Intelligence facilitates the effectiveness of ISMS for the following reasons:

- “Big Game Hunting” – Adversaries are focusing more and more on a specific target instead of running broad attack campaigns, which incidentally leads to more sophisticated attacks.[1]
- Malware-free attacks and increasing use of “Living off the Land” techniques[2]
- Professional malware business models of criminal groups[3]
    - e.g. Emotet-Trickbot
    - sharing of compromised credentials and data
- Energy sector companies can be a high-level target for criminal groups as well as nation state sponsored groups[4]
- IT and OT security should always be considered together[5]

This paper explicitly addresses the needs of small and medium enterprises (i.e. enterprises with a headcount of less than two thousand employees and cyber security departments with a headcount of one to five) in the energy sector which are planning to use Threat Intelligence to improve detective and reactive cyber security controls in their organization.

[1] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/01/30/the-cybersecurity-202-u-s-adversaries-are-raising-their-cyber-game-intel-officials-warn/5c509c2d1b326b29c3778d02/
[2] https://www.cpomagazine.com/cyber-security/malware-free-attacks-step-up-the-pace/#:~:text=According%20to%20CrowdStrike%2C%20malware%2Dfree,are%20exploited%20for%20remote%20logins
[3] https://www.paloaltonetworks.com/resources/research/ransomware-report
[4] https://www.hornetsecurity.com/en/security-information/cybersecurity-special-energy-sector/
[5] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Definitions

Cyber Threat Management

"Cyber Threat Management (CTM) is emerging as the best practice for managing cyber threats beyond the basic risk assessment found in ISMS. It enables early **identification of threats**, **data-driven situational awareness**, **accurate decision-making**, and **timely threat mitigating** actions.

CTM includes:

- Manual and automated intelligence gathering and threat analytics
- Comprehensive methodology for real-time monitoring including advanced techniques such as behavioural modelling
- Use of advanced analytics to optimize intelligence, generate security intelligence, and provide Situational Awareness
- Technology and skilled people leveraging situational awareness to enable rapid decisions and automated or manual actions"[6]

Threat Intelligence

"Threat Intelligence is **evidence-based knowledge**, including **context**, **mechanisms**, **indicators**, implications and **actionable advice**, about an existing or emerging menace or hazard to assets that can be used to **inform decisions** regarding the subject's response to that menace or hazard."[7]

Tactics, Techniques and Procedures (TTPs)

Tactics, Techniques and Procedures (TTPs) is an essential concept in cyber security and describes the behaviour of a threat actor or group. It is a term taken from the traditional military sphere and is used to characterize what an adversary does - and how - in increasing levels of detail.

For instance, a tactic might be using malware to steal credit card credentials. A related technique (at a lower level of detail) might be sending targeted emails to potential victims; these emails have documents attached containing malicious code which executes upon opening, captures credit card information from keystrokes, and uses http to communicate with a command and control server to transfer information. A related procedure (at a lower level of detail) might be to perform open source research to identify potentially gullible individuals, then craft a convincing socially engineered email and document, create malware/exploit that will bypass current antivirus detection, establish a command and control server by registering a domain called mychasebank.org, and send mail to victims from a Gmail account called accounts-mychasebank@gmail.com.

TTPs consist of the specific adversary behaviour (attack patterns, malware, exploits) exhibited, resources leveraged (tools, infrastructure, personas), information on the victims targeted (who, what or where), relevant exploit targets being targeted, intended

[6] https://en.wikipedia.org/wiki/Threat_(computer)#Threat_management
[7] https://www.gartner.com/en/documents/2487216

effects, relevant kill chain phases, handling guidance, source of the TTP information, etc.

TTPs play a central role in cyber threat information and Cyber Threat Intelligence (CTI). They are relevant for indicators, incidents, campaigns, and threat actors. In addition, they have a close relationship with exploit targets characterized by the specific targets that the TTPs seek to exploit.[8]

Indicators of compromise (IoCs)

Indicators of compromise (IoCs) are pieces of forensic data, such as data found in system log entries or files that identify potentially malicious activity on a system or network. Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damage by stopping attacks at earlier stages.

Examples of indicators of compromise are unusual outbound network traffic, anomalies in privileged user account activity, unusual DNS requests, etc.[9]

Operational Technology, ICS, PLC and SCADA

Operational Technology encompasses the computing systems that manage industrial operations. This includes monitoring of the Electric Utility Grid and more.

ICS is an umbrella term that includes both SCADA and DCS. An ICS network can monitor many infrastructures and raw material systems.

SCADA is a system architecture for managing large and complex processes. SCADA systems consist of three main components:

1) central command centre
2) local control systems
3) communication systems

Distributed Control System (DCS) is a type of process control system that connects controllers, sensors, operator terminals and actuators. The data acquisition and control functions are performed by distributed processors situated near the peripheral devices or instruments from which data is being gathered. A PLC, on the other hand, is designed to actually control the devices in its immediate surroundings based on the PLC programming.

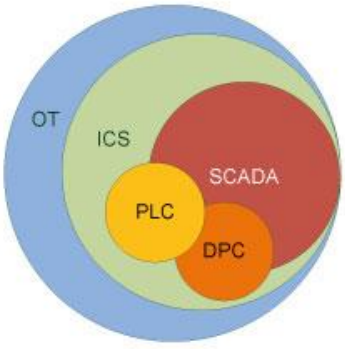


Figure 1: Operational Technology. Source: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

[8] https://stixproject.github.io/data-model/1.2/ttp/TTPType/
[9] https://digitalguardian.com/blog/what-are-indicators-compromise

Threat Intelligence Management

To benefit from Threat Intelligence, an organization must have a basic maturity in its cyber security. Otherwise, it will not be able to utilize Threat Intelligence.

Foundation - Before Threat Intelligence is put on the agenda, the organization should have an asset inventory, know about vulnerabilities and carry out risk assessments. With these requirements met, intelligence management will allow threat modelling, mitigation and all the other benefits.

The Threat Intelligence Management Process itself covers the following phases, which describe the Intelligence Lifecycle.

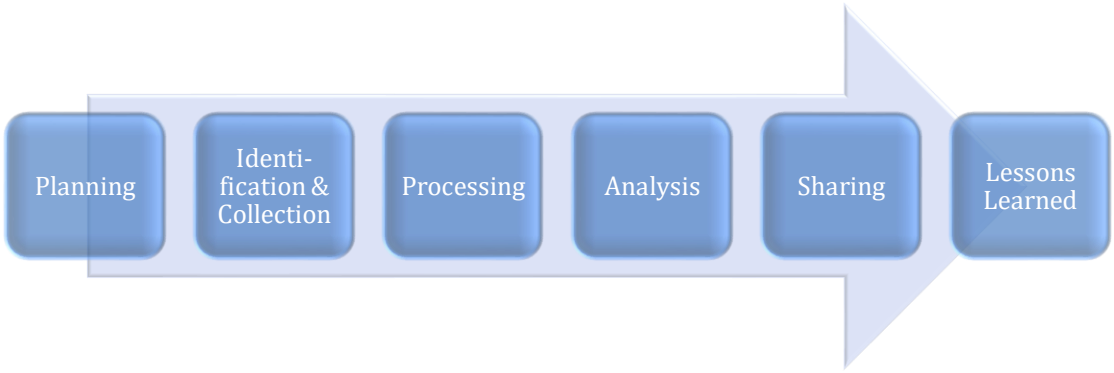


Figure 2 Threat Intelligence Management Process.

Planning – The requirements for Threat Intelligence Management need to be defined. The work product of this phase should be documented and realistic goals. This work product may equally serve as a briefing paper for employees supporting the following phases.

Identification and Collection – Utilities are granted access to a variety of intelligence sources from authorities, national cyber security centres, ISACs and commercial intelligence services. Proper identification does not aim to maximize the Threat Intelligence being collected, but rather to collect the right intelligence with the following characteristics:

- it supports the goals as described in the planning phase
- it can be consumed and made usable by the organization
- it has been collected in a structured way following establishment of data collection mechanisms (e.g. OT SOC)

Processing – In this phase, Threat Intelligence raw data is converted into useful information (intelligence). For instance, this can be achieved by grouping data, bringing it into a structured format that can be pivoted, etc.

Analysis – In this phase, the intelligence from the processing phase is used to generate intelligence reports. The intelligence reports contain correlated information from different sources. The analyst adds his personal conclusion and overall takeaways. The report must be adapted to the recipient's needs (e.g. PowerPoint for Management).

Sharing – Intelligence reports in the energy sector become more effective if they are shared between utilities. Yet, data from the ICS is often sensitive data, and the producer is reluctant to share it. The EE-ISAC offers a solution by providing a network of trust for the energy sector in Europe.

Lessons Learned – Analysts and Consumers should regularly evaluate the usefulness of the intelligence reports. This requires communication between these two parties, and does not follow a waterfall model but instead is ongoing, back and forth.

Foundation: The Asset Inventory and where to go from here

Asset Inventory

Asset inventory is a database which lists and provides details of the assets an organization or company owns. Through the asset inventory management process, all the assets are monitored in order to examine issues such as physical location, maintenance requirements, depreciation, performance and eventual disposal of the asset.

When an organization needs to make sure that its assets are being used efficiently, it should take the below key features into consideration:

- **good maintenance scheduling** – Plan and arrange both routine/emergency repairs to equipment and maintain the asset inventory in order to eliminate business disruptions.
- **good reporting** – Analyze different aspects of the asset inventory in order to track and compare performance.
- **easy configuration and customization** – Adjust workflows, template documents and forms to suit the organization's processes and policies.
- **Asset location and data accessed** – Vulnerability scans should be compared against the asset inventory to detect potential discrepancies.

Vulnerability/Threat Monitoring, Filtering and Identification

The objective of this step is to prepare in advance a list of potential threats. This involves security analysts using vulnerability databases, vendor vulnerability announcements, asset management systems and Threat Intelligence feeds to identify and test security flaws on applications, servers or other systems.

Cyber Security Risk Assessment

Risk assessment is a crucial part of a company´s or organization's threat management strategy. During this step, all the information assets that could be affected by a potential attack, such as customer data, hardware, intellectual property, etc., are identified, as well as the risks that could affect those assets. Also, a risk estimation and evaluation are usually performed, after which controls are selected to manage the identified risks. In the light of the above, it is important to monitor and review the risk environment continuously to detect any changes in the context of the organization and to maintain an overview of the complete threat management process.

Threat Modelling and Prioritizing

The next step is to assess the severity of the vulnerabilities for specific use cases and then prioritize their remediation. Threat modelling uses the asset inventory to determine which assets are the most valuable to the organization and which threats pose the highest risk to the high-value assets. Depending on the severity of each potential threat, certain criteria can be checked and analyzed, such as the impact of each threat, the assets it can affect and its potential vectors.

Analysis & Remediation Planning

An organization should be able to analyze and verify that attack vectors are eradicated and take action to prevent similar attacks in the future. Collaboration and documentation sharing among users and across teams is advised. It is essential that

the information is distributed among the interested communities and that solutions are suggested.

Mitigation

The final step is the mitigation of the identified vulnerabilities/threats. Some mitigation steps may be temporary measures, such as notifying customers and requiring them to take a unit offline or change its configuration until a patch can be issued. Other mitigation steps can be more involved, requiring development work, incorporating new versions of components into the system, testing, issuing updates and so on. At this point, the root causes of incidents must be eliminated or at least minimized, and businesses, functions, IT and stakeholders should return to a secure operating environment.

Asset Identification & Network Security Monitoring

One important step of actionable Threat Intelligence is to gather raw data that fulfils the scope and business requirements in terms of implementing Threat Intelligence.

An optimal solution is to collect data from a wide range of sources, ranging from publicly available information to CTI platforms like MISP (see chapter MISP). An organization can have many different external sources for collecting data, either paid or free. Some of these sources originate from the open web, the dark web, or technical sources, such as feeds from companies, CTI platforms and national reports. Data can be also collected via internal sources, such as network event logs and records of past incident responses, etc.

Besides the sources, the structure of the data collected for further processing and analysis at a later stage is also of importance. Threat data is usually thought of as lists of IoCs, such as malicious IP addresses, domains, and file hashes, but it can also include vulnerability information, like the personally identifiable information of customers, raw code from paste sites, and text from news sources or social media. The SIEM of the organization may be a central point for collecting, storing and reconciling such data.

Although this paper focuses on using external Threat Intelligence, we encourage the use and combination of both external and internal Threat Intelligence and, furthermore, utilization of the data already held in the infrastructure of your organization.

ICS events are an example of a source of information collected internally. The information gathered should comprise the following categories:

- MAC/IP addresses
- Manufacturer information
- Device type and role
- Model number
- Firmware/software revision
- Configured and active services
- Device-level diagnostic and prognostic details
- Performance data
- Event logs

Collecting ICS events can be accomplished with different methods. Most of these methods are passive and thus have minimal impact on the ICS system. As an example, network switch port monitoring gives valuable information about the network communication of your ICS. Apart from gathering events from network elements as switches, valuable information about the operation of the industrial network can also

be obtained from the supervisory devices. Such devices in ICS systems are the Engineering Workstation, the HMI and SCADA systems as well as the Historian. The information from endpoints can be even more valuable than information on the networks, as they can provide a true wealth of information. Many vendors allow and support the deployment of agents to extract logfiles and forward these to a SIEM (examples of free and proven tools are NXLog or BEATs).

However, in addition, active techniques have emerged recently that are trying to obtain information from ICS devices by scanning or polling methods.

Polling consists in using scanning libraries to obtain information about the industrial network that cannot be easily extracted through passive monitoring or from the endpoint events. Such information is related to the device role or diagnostic information. Scanning methods include using libraries such as Nmap or fingerprinting engines as a scanner (https://github.com/kudelskisecurity/scannerl) to obtain information, and polling methods rely on messages for PLCs and RTUs formatted according to the proprietary industrial protocols that are also used by Engineering Workstations.

This practice is usually avoided by ICS operators, as scanning can cause performance issues in ICS devices or even take down certain operating devices.

The ideal strategy for collecting internal Threat Intelligence is to use a hybrid passive monitoring and active polling method, in which most of the information is obtained passively and the remainder can be obtained by polling in the same way as an Engineering Workstation.

The identified and validated assets, networks and their topology should be visualized. Applications, services and how they interact should be documented.

Planning: Organizations' Requirements for Threat Intelligence

The development of requirements for Threat Intelligence is the first phase of the intelligence cycle. Here, an organization will ensure that use of Threat Intelligence meets the needs of the security program.

The requirements of the organization should be determined and realistic goals should be derived. The goals should be formalized in such a way that they can be easily explained and understood by the recipients, e.g. Management, Incident Responders and CERT employees.

More and more organizations are specifying requirements. Organizations which have not yet formalized this process can start by identifying the teams who leverage CTI. Once the teams have been identified, the organization can question them regarding any ambiguities or problems they are consistently encountering that CTI could help address.

Examples of requirements from respondents include:

- The activity of a specific adversary with whom we had security incidents in the past: the CTI team is tasked with monitoring for new reported activity as well as profiling the observed TTPs of this adversary
- Brand surveillance, supply chain and partner assessments

The most common threat management priorities are to improve threat detection, support proactive threat hunting, improve the investigation and the analysis for threats and to improve lateral movement detection.

Be sure to consider cyber security barriers that could affect the Threat Intelligence Management, e.g. the lack of trained staff or the lack of budget.

Many organizations in the energy sector have dedicated resources for CTI that are typically members of the security operations centre or the incident response team.

Furthermore, it may be beneficial to define metrics of Cyber Threat Intelligence during the Planning phase. Even though there are no one-size-fits-all KPIs, performance measurement should be embedded in the typical Threat Data scenarios, e.g. Detecting Threats and Attacks, Incident Response or Vulnerability Management.

Threat Intelligence could be measured by

- **Completeness –** Do I have sufficient details for my response?
- **Accuracy –** Can mistakes be reduced?
- **Relevant –** Are threats relevant to your organization addressed and details delivered in a consumable manner?
- **Timely –** Is it delivered quickly enough?

Data Collection

In the Data Collection phase, you will specify where and how to acquire data, information or other intelligence. This phase needs to be considered substantial, due to the implications in the following process phases.

Based on the SANS Threat Intelligence Survey in 2020, the following CTI data was gathered by the respondents (cross-industry).

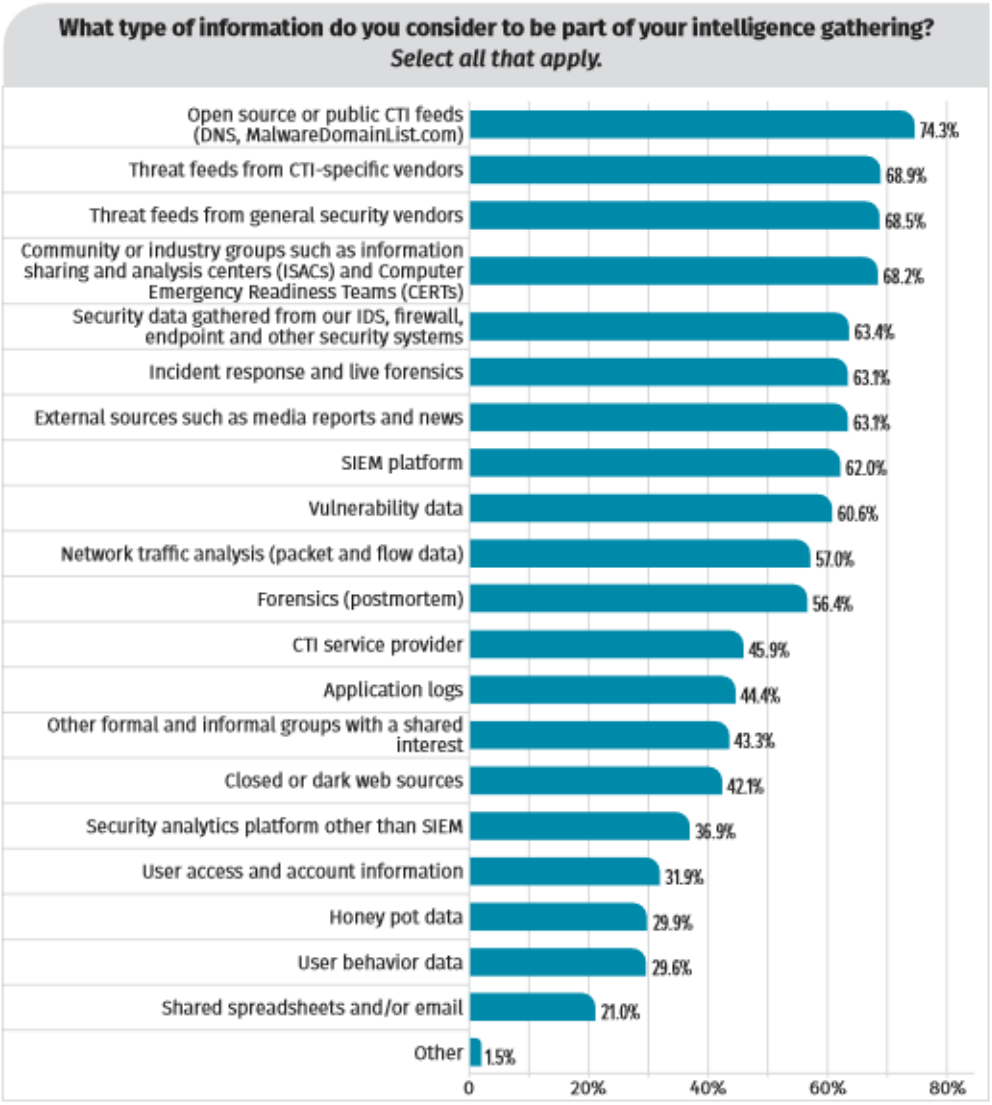


Figure 3: Result of survey for intelligence gathering. Source: https://lp.threatq.com/rs/619-ADG-031/images/Survey_CTI-2020_ThreatQuotient.pdf, Figure 9

The data sources that should be used depend on the organization´s need (Detection, Prevention, Response or Mitigation) and the recipient (Management, SOC, IR-Teams).

One interesting trend in collecting Threat Intelligence in regard to both data and tools is the use of open source platforms, for instance threat feeds as a collection source or Threat Intelligence Management tools like Collaborative Research Into Threats (CRITs) and Malware Information Sharing Platform (MISP, see chapter MISP). Another trend is an increased emphasis on attacker TTPs rather than just IoC aggregation (see chapter MITRE ATT&CK).

For the energy sector in general, the external Threat Intelligence Sources from ICS-CERTs and ISACs (as also described in the MISP section) are considered essential and beneficial.

The need for CTI within an organization may change over time and may be rather threat-centric, team-centric or tool-centric, depending on the organization's needs.

For organizations with a lower cyber security maturity, it makes sense to focus on a few TTPs, rather than loading excessive numbers of IoCs.

Processing

Data must be processed before it can be analyzed and turned into intelligence. Processing includes repeatable tasks such as deduplication of data, data enrichment and data standardization, along with other more intensive tasks requiring analysis of their own, like reverse engineering of malware[10].

Processing is typically a manual or semi-automated process phase.

The majority of external CTI data comes pre-processed and does not require processing within your organization. TTPs are an example of this. Also, security data gathered automatically from your security components (firewalls, IDSs), do not need to be considered as they are processed automatically in the respective security solutions.

Processing should be a focus point in the work with your SIEM and the data loaded into the SIEM by your assets. Processing focus points include data correlation and data enrichment; both should be continuously ongoing tasks following documented procedures.

Maltego Threat Analysis

Threat analysis is the process of extracting intelligence from information and data. This is achieved by combining historical views, real-time data and upcoming trends and linking them to the criticality for the business. The goal is to be able to make fact-based decisions regarding the incident response process. An asset inventory and an understanding of which business processes are dependent on which IT assets are crucial to a good threat analysis process.

Linking different information and data together to bring threats into a context:

- Information about adversaries (TTPs)
- IoCs from threat feeds / malware analysis
- IoCs from own SOC analysis
- Internal asset database / network infrastructure
- Status of vulnerabilities in IT assets
- Internal security monitoring

The goal of Threat Intelligence is to make information available to the analysts that helps them in the mitigation of potential incidents. There are several levels of Threat Intelligence that vary in their complexity, ability to be shared and the comprehensiveness of the information. This is depicted very well in the “pyramid of pain in Threat Intelligence” which separates the various types of intelligence available. While Tactics, Techniques and Procedures (TTPs) are the most abstract type of information available, they need the most additional effort to be applied to actual incidents. On the other hand, IP addresses and hash values can be easily shared and applied, but reveal little about how an adversary acts.

For each of the levels of the pyramid, a different set of tools and applications can be utilized to optimally address the different challenges in each level. In this paper, the

[10] https://lp.threatq.com/rs/619-ADG-031/images/Survey_CTI-2020_ThreatQuotient.pdf

lower level of concrete evidence, such as domain names and IP addresses, is addressed through the MISP platform later in the tools sections, whereas higher levels are covered via the MITRE ATT&CK framework.

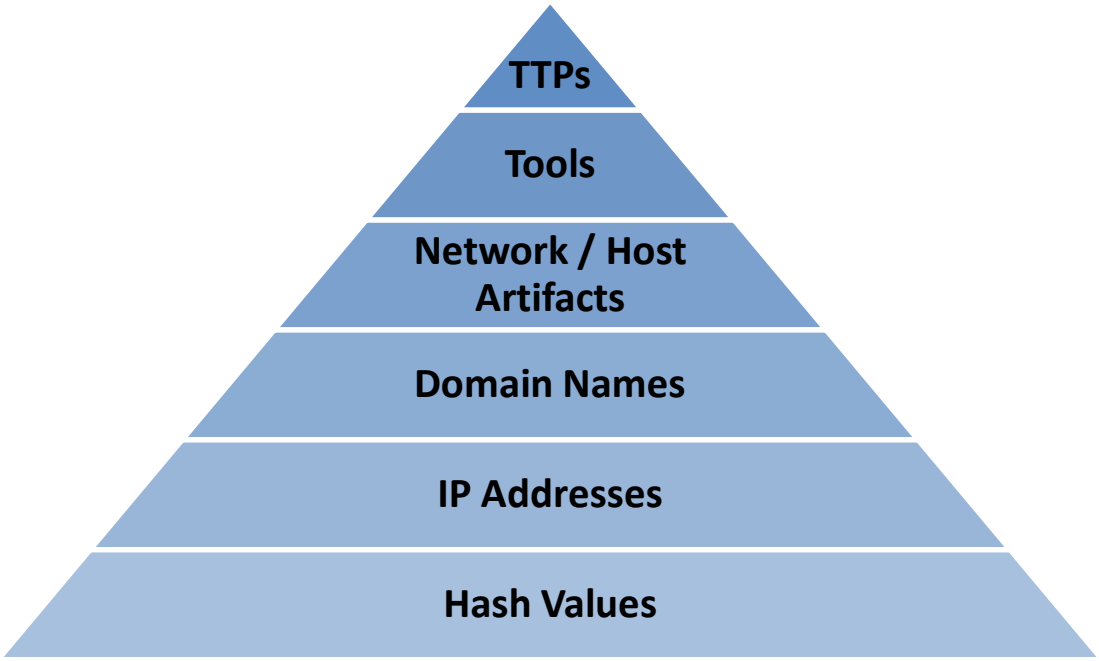


Figure 4: Pyramid of Pain in Threat Intelligence.

Reporting/Visualization/Sharing

Even the best-analyzed CTI products become ineffective if they are not provided to the right audience in a timely manner.

The right stakeholder has to be addressed with the right message. The most common methods utilized for dissemination are emails, documents, spreadsheets, PowerPoint or briefings. A rich and complete data structure for reporting, visualizing and sharing such information that includes impact, threat vectors, affected assets, geographical spread and categorization according to threat taxonomy should be considered. A Threat Intelligence platform may be supporting all dissemination activities.

For each recipient it should be ensured that CTI helps to reduce mean time to recovery, shorten dwell time of the adversary and give guidance on what to focus on to reduce risks (e.g. vulnerabilities, news, adversaries).

Interfaces – Incident Response and Security Operations

Incident Response (IR) and Security Operations should provide input for cyber threat management and vice versa. After resolving an incident, all IR documentation and artefacts are analyzed by CTI. The extracted intelligence information is then passed to the SOC to enhance further security operations such as monitoring and detection.

IR can provide valuable information for CTI:

- Root causes and initial attack vectors can reveal weaknesses
- New IoCs and TTPs for known threats
- Lateral movement techniques for enhancement of monitoring and detection capabilities

- Actions on objectives of threats

CTI can help IR:

- List of current threat actors and typical TTPs concerning a given company and asset inventory
- Linking observable events to possible threat actors (further information for TTPs)
- Playbooks to cope with known attacker procedures

CTI input for SOC:

- New data sources that need to be incorporated into SIEM
- Necessary queries and alarms
- Information on evasion techniques for existing security, monitoring and detection measures

Overall, the linkage between IR, SOC and CTI is most beneficial when realized at a tactical level and should not be seen as a major strategic effort. Small specific improvements in daily routines can lead to quick wins.

Interfaces – C-Level (Investment / Threat / Requirement)

To make use of Threat Intelligence for the board and senior decision makers, a recommended approach is to manually compile the most relevant intelligence on two to three PowerPoint slides.

For management, strategic analysis of the adversary and the digital footprint or attack surface might be of more relevance than for other stakeholders, as the risk assessment can be based on this data. The resources allocated to the cyber security organization and the CTI department are derived from this assessment. Management's question "Do my investments match my threat landscape and requirements?" should be answered by CTI.

Tools

Maltego

Maltego is a data mining tool that mines a variety of open-source data resources and uses that data to create graphs for analyzing connections. The graphs assist analysts in visualizing threat infrastructure through link/node connections and allows for multiple data sources to be combined into a single interactive graph. This tool can be especially helpful when analyzing a complex infrastructure by visually aiding analysts in connecting disparate data sets.

There are several versions of Maltego available:

- Maltego XL- Premium version for large data
- Maltego Classic- Pay version which includes all APIs (transforms)
- Maltego CE- Free Version with limited APIs (transforms)
- Casefile- For examining links in offline data

Maltego is a perfect platform for watching social media conversations unfold. With the added advantage of importing targets directly into Maltego for follow-up research or

targeting, it is possible to track social media or to find key hashtags and users involved in the spread of information around an event or topic.

Within the machine's tab, by selecting the "Run Machine" icon, it is feasible to choose the intended target and start exploring. For example, by using a phrase to find tweets, select "Twitter Monitor." As a result, the input will be phrases that are expected to be in a conversation.

Once you start your machine, it will take a while to fill the graph with the information. This may take a few minutes of Maltego running new iterations to pull in more data. The information you see in the graph may be overwhelming, so it's good to "set layout mode to Organic" from the Layout section in the toolbar on the left of the graph.[11]

Figure 5: Maltego UI.

MISP

The Malware Information Sharing Platform is a Threat Intelligence platform for sharing, storing and correlating a variety of information, covering:

- Indicators of Compromise (IoC) of targeted attacks
- General Threat Intelligence or information including actionable artefacts, such as IP or domain names
- File hashes (e.g. for malicious files)
- Aggregated information, such as financial fraud information
- Vulnerability information or
- Counter-terrorism information

The platform is used in multiple organizations, often in multiple instances in relation to the same information and is used internationally to share and distribute information about threats and how to detect and identify them. Originating from a personal project, it has subsequently been used and promoted by the military in Belgium and later NATO. The Computer Incident Response Centre Luxembourg took care of its development and distributes it as open source software.

[11] Part of the information provided on the Maltego tool was supplied through the GDL09-Aviation-Cyber-Threat-Briefing (TLP GREEN) of EATM-CERT from Eurocontrol.

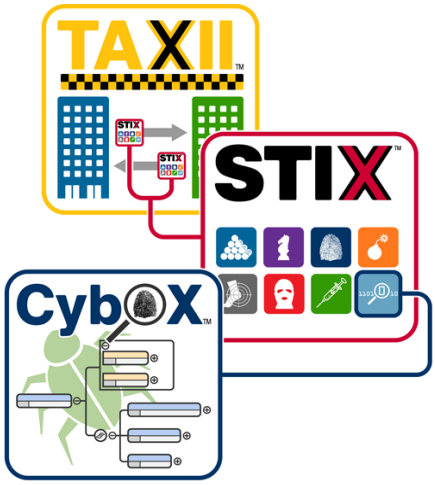
MISP solve a variety of important problems in addressing cyber security threats in large organizations, namely by:

- Receiving timely updates and information about currently known threats
- Obtaining this information from various sources
- Integrating correlation into the database to identify which information is already available
- Integration into various other tools in cyber defence, either directly (using modules, the API or the data model) or via use of open formats
- Utilization of commonly available knowledge bases, such as MITRE ATT&CK

Figure 6: MISP Threat Information Sharing. Source: www.misp-projekct.org

Generally speaking, by using MISP, an organization is able to consume a number of threat alerts via feeds, which can be available free of charge or via paid subscriptions, and then use the correlation and input capabilities of MISP to connect this data with information from its own network and gain previously unknown insights. Depending on the maturity of the cyber security within the organization, e.g. the availability of dedicated threat hunting teams, multiple instances can be used for data separation based on the availability of feeds (public/commercial), additional feature usage (e.g. sightings API) and/or the confidence of the data stored in the instance (low volume but confirmed TI vs. high volume but unconfirmed TI).

STIX and TAXII



The ability to quickly share and distribute threat-related information plays an important role and, alongside correlation, is the most important feature of MISP.

A set of protocols and formats have been developed to facilitate this sharing activity.

At the bottom, the Trusted Automated eXchange of Indicator Information (TAXII) protocol enables HTTPS-secured exchange using various sharing models, using possible different collections and channels to receive and share information in an application-agnostic way. Several organizations already offer their data via TAXII, e.g. CISA.

On top of TAXII as a protocol to transport the data between points, the structured threat information expression language (STIX), which in the current version also includes the

cyber observable expression (CybOX), is used to serialize and express the easy and complex relationships the TI data might have, and to transport this complexity between endpoints. A variety of objects can be deployed to make use of this language, such as Indicators, Identity, Attack Pattern, Threat Actor, Report and many more.

Ensuring that security products, especially those in use at the perimeter, understand either TAXII for transport or STIX to incorporate received data, could be a valid requirement for software procurement.

MITRE ATT&CK

Published by the MITRE Corporation, the ATT&CK acronym stands for the Adversarial Tactics, Techniques, and Common Knowledge framework; this already describes its primary objective, which is to divide the information into manageable parts and to be able to classify these parts.

Figure 7: MITRE ATT&CK framework. Source: https://attack.mitre.org/

It therefore enables users to concentrate and focus on the specific tactics attackers are currently using, or have used, for attacks (successful or failed).

The amount of information that has to be classified is understandably vast and distinct, and therefore the classification has to be rather comprehensive as well, as shown in the MITRE ATT&CK MATRIX (figure 7). In order to act as a very valuable tool for creating kill chains, it needs to be fed with information to produce useful results. It is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security product and service community.

As mentioned at the beginning of this document, the level of additional value an organization can obtain by applying Threat Intelligence is correlated to the level of

maturity this organization already has. So while the MITRE ATT&CK framework could already be useful for a security operation that is being ramped up, e.g. via focusing on certain classes that are most interesting, the additional value becomes evident once this operation reaches a certain level in terms of expertise and available resources.

One applied example is available from the MITRE ATT&CK blog, showing the potential of the classification during the analysis of a report (figure 8).

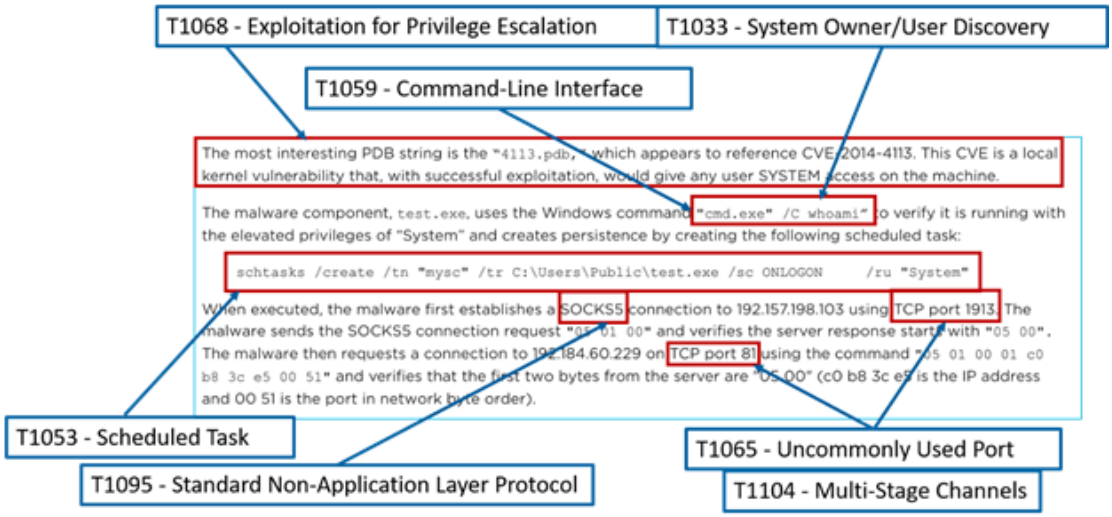


Figure 8: Example report mapped to MITRE ATT&CK (MITRE official blog)

As shown, the natural language of the report is translated into the various classes of the framework which in return can provide additional insight about which measures are available in the organization to counter the reported threat or to identify gaps in the security concept.

This is still a reactive approach that requires a report to be published first and then analyzed, but with more means for detection, the MITRE ATT&CK framework can be utilized for prospective purposes as well. Having an overview of the specific techniques used by specific adversaries whom perimeter logs confirm as having been potentially active can reveal whether the preparations are sufficient to detect this group, or whether there are potential loopholes that could be addressed before primary defences are breached. The ATT&CK navigator[12] has been designed to facilitate this process.

Of course, not all systems are the same, and from both the attackers' and defenders' perspective, the approach differs depending on whether an enterprise, a mobile or an industrial network needs to be addressed. This is also reflected in the various matrices available, where each of the aforementioned types has its own matrix, with many classes overlapping but with a different emphasis and implementations. Most notably, the number of classes is different, which reflects the more limited ICS and mobile environment. Usually, the matrices should be used according to the addressed systems, which are often mixed. So while the Microsoft Windows-based operator workstations should be addressed with the enterprise matrix, the more specialized industrial equipment should be covered by the ICS matrix, whereas mobile devices used by field personnel adhere to the classes of the mobile matrix.

[12] MITRE ATT&CK navigator, https://mitre-attack.github.io/attack-navigator

ATT&CK® for Industrial Control Systems

Attacks on ICS require substantial effort and sophisticated actions by adversaries due to the presence of proprietary hardware, software and communication protocols as well as the specific characteristics of each process. Nevertheless, adversaries are attracted to targeted attacks against them since they have a massive impact on the physical world and catastrophic consequences. The consequences of abnormal operation in ICS include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial consequences such as production losses, negative impact on a nation's economy, and compromise of proprietary information.

The actions taken by adversaries for EPES systems involve several tactics, techniques and procedures that are listed by MITRE as the ATT&CK for ICS framework. In contrast to the ATT&CK for Enterprise MITRE framework, in which only security risks are considered, ATT&CK for ICS is also linked with the safety risks of the ICS system. The focus is on tactics because they define how the adversaries are performing their actions on the ICS system. The tactics are visualized in a pyramid schematic due to the level of the ICS system to which they are applicable, i.e. initial access techniques are usually applicable to the enterprise network or supervisory ICS devices, whereas disruption techniques are usually applicable to field devices such as industrial controllers (PLCs). The levels of ICS systems are identical to the ICS systems themselves, and use the Purdue Model to segment their architecture. It is important to note that this complexity is not to be confused with the difficulty of an adversary using one of these tactics in an ICS system. ICS systems have 11 associated categories of tactics:

- Initial Access, defining how an adversary gains initial access on the EPES system.
- Execution, defining how an adversary can execute malicious code on the EPES system.
- Persistence, defining how an adversary maintains access on the EPES system.
- Evasion, defining how an adversary fools the operator or existing security mechanisms into thinking that the system behaviour is normal and no attack is present.
- Discovery, defining how an adversary locates the devices that impact the industrial process.
- Lateral Movement, defining how an adversary can move inside the EPES system to reach devices that impact the industrial process.
- Collection, defining how an adversary is trying to gather data of interest and domain knowledge on the targeted ICS environment to inform their goal.
- Command & Control, defining how an adversary communicates with external servers to receive malicious data that will cause disruption of EPES devices as well as the industrial process.
- Inhibit Response Function, defining how the adversary tries to overcome the safety protection schemes that are in place for processes and products of the industrial system.
- Impair Process Control, defining how the adversaries can trigger physical impacts on the system (e.g. stop/degrade the process or cause catastrophic failure).
- Impact, defining how the adversary is trying to manipulate, interrupt or destroy the ICS systems, data and their surrounding environment.

The ATT&CK for ICS framework can be used to better characterize and describe post-compromise adversary behaviour within the ICS domain. Concerning threat management, it can also be a tool to develop ICS-specific threat models and methodologies which can be used to evaluate counter-measures or act as a guide for threat hunting within OT networks.

In more mature security operations, the framework can be integrated in your SOC Systems for classification and correlation purposes (e.g. ATT&CK Navigator combined with MISP and documentation/ticket systems like The HIVE)

MITRE DETT&CT for Blue Teams

DeTT&CT[13] delivers a framework which does exactly that and it will help in the administration of blue teams' data sources, visibility and detection. It also provides the means to administer Threat Intelligence from an organization's own intelligence team or third-party provider. This can then also be compared to current detection or visibility coverage.

OpenCTI Platform

OpenCTI[14] is an open source platform allowing organizations to manage their Cyber Threat Intelligence knowledge and observables. It has been created in order to structure, store, organize and visualize technical and non-technical information about cyber threats.

The goal is to create a comprehensive tool allowing users to capitalize technical (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology etc.) while linking each piece of information to its primary source (a report, a MISP event, etc.), with features such as links between each information, first and last seen dates, levels of confidence etc. The tool is able to use the MITRE ATT&CK framework (through a dedicated connector) to help structure the data. The user can also choose to implement its own datasets.

OpenCTI is a product powered by the collaboration of the French national cyber security agency (ANSSI), the CERT-EU and the Luatix non-profit organization.

AbuseHelper

AbuseHelper[15] is an open-source project initiated by CERT.FI (Finland) and CERT.EE (Estonia) with ClarifiedNetworks to automatically process incident notifications.

This tool is being developed for CERTs (and ISPs) to help them in their daily job of following and treating a wide range of high-volume information sources. The framework can also be used to automatically process (standardized) information from a wide range of sources, e.g. feeds from servers (e.g. shadow server) to provide comprehensive information about vulnerabilities.

[13] https://github.com/rabobank-cdc/DeTTECT/wiki
[14] https://www.opencti.io/en/
[15] https://github.com/abusesa/abusehelper

IntelMQ

Originally influenced by AbuseHelper, the IntelMQ[16] is a solution for the security team and aims to improve automation, not only for incident handling, but also for situational awareness and notifications. IntelMQ is part of a community-driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several InfoSec events.

As a message queue (MQ) for Threat Intelligence (Intel), it depicts a system which utilizes bots – encapsulated functional blocks working on a specific part within the queue – to divide the problem of automated Threat Intelligence handling into manageable parts. Each bot collects, parses, enriches or outputs information and can be concatenated with others to achieve queue-like processing.

This enables IntelMQ to take feeds such as those from the previous tools and create their output in an .xml or other file format that can be further processed in different systems and thus help to handle the available amount of data.

Hackmageddon

Hackmagedddon[17] is a platform which provides Cyber Attacks timelines for certain periods. Users can add an attack to the Cyber Attacks Timeline of the corresponding period and contribute as a community to the creation of these timelines.

Thor - APT Scanner

THOR[18] is the most sophisticated and flexible compromise assessment tool on the market.

Incident response engagements often begin with a group of compromised systems and an even bigger group of systems that may possibly be affected. The manual analysis of many forensic images can be challenging.

THOR speeds up your forensic analysis with more than 10,000 handcrafted YARA signatures, 400 Sigma rules, numerous anomaly detection rules and thousands of IoCs.

THOR is the perfect tool to highlight suspicious elements, reduce the workload and speed up forensic analysis at moments in which getting quick results is crucial.

Tooling according to the TI phases

Tool	Phases
Maltego	- Threat Modelling and Prioritising
MISP	- Vulnerability/Threat Monitoring - Filtering and Identification

[16] https://github.com/certtools/intelmq
[17] https://www.hackmageddon.com
[18] https://www.nextron-systems.com/thor/

STIX and TAXII	- Analysis & Remediation Planning - Mitigation
MITRE ATT&CK	- Vulnerability/Threat Monitoring, Filtering and Identification - Threat Modelling and Prioritizing - Analysis & Remediation Planning - Mitigation
OpenCTI platform	- Vulnerability/Threat Monitoring, Filtering and Identification - Threat Modelling and Prioritizing - Analysis & Remediation Planning - Mitigation
AbuseHelper	- Vulnerability/Threat Monitoring, Filtering and Identification - Analysis & Remediation Planning - Mitigation
IntelMQ	- Vulnerability/Threat Monitoring, Filtering and Identification - Threat Modelling and Prioritizing - Analysis & Remediation Planning - Mitigation
Hackmageddon	- Vulnerability/Threat Monitoring, Filtering and Identification - Analysis & Remediation Planning - Mitigation
Thor - APT Scanner	- Vulnerability/Threat Monitoring, Filtering and Identification - Threat Modelling and Prioritizing - Analysis & Remediation Planning - Mitigation

AI and Automation in CTM Solutions

A lot of solutions and tools for CTM advertise their use of artificial intelligence or automation of workflows and decisions. On the one hand, this can be very beneficial in coping with repeatable tasks in huge environments, but on the other hand, AI and automated decisions can be a problem within CTM and IR. In many use cases requiring decisions, such as alarms or prioritization, you need to know what rules have led to a specific result in order to find root causes or to identify false positives. These kinds of conclusions are not possible with AI technologies or black box solutions provided by vendors who want to protect their algorithms and functions.

It is recommended to test those solutions in relation to the aforementioned restrictions for your specific use case.

Recommendations & Conclusion

Effective Threat Intelligence Management will make cyber security operations more efficient and will improve your return on investment in cyber security. Threat Intelligence should not be prepared only for SOC/IR staff, but should be circulated at all levels of the organization, to executives, risk managers and security experts.

There is plenty of free information available in the public domain that can be used. Harvesting this intelligence is not necessarily associated with large investments.

Authorities and bodies like the EE-ISAC should be used as a starting point to ensure that the most relevant Threat Intelligence is handled by your organization.

Acknowledgements and Contact Details

This white paper has been produced with the support of EE-ISAC members.

EE-ISAC
Alexander Harsch
E.ON SE

Alexander.Harsch@innogy.com

EE-ISAC
Marcel Kulicke
Siemens

Marcel.Kulicke@siemens.com

EE-ISAC
Christina Skouloudi
Konstantinos Moulinos
Antigone Zisi
ENISA

Konstantinos.Moulinos@enisa.europa.eu
Christina.Skouloudi@enisa.europa.eu
Antigone.Zisi@enisa.europa.eu

Andreas Seiler
LEW

Andreas.Seiler@lew.de