Towards Mitigation of Data Exfiltration Techniques using the MITRE ATT&CK Framework*

Michael Mundt[1] and Harald Baier[2,3]

[1] Esri Deutschland GmbH, Bonn, Germany
[2] Universität der Bundeswehr München, Germany
m.mundt@esri.de
https://www.esri.de
[3] Research Institute CODE, Universität der Bundeswehr München, Germany
harald.baier@unibw.de
https://www.unibw.de

Abstract. Network-based attacks and their mitigation are of increasing importance in our ever-connected world. Besides denial of service a major goal of today's attackers is to gain access to the victim's data (e.g. for espionage or blackmailing purposes). Hence the detection and prevention of data exfiltration is one of the major challenges of institutions connected to the Internet. The cyber security community provides different standards and best-practices on both high and fine-granular level to handle this problem. In this paper we propose a conclusive process, which links Cyber Threat Intelligence (CTI) and Information Security Management Systems (ISMS) in a dynamic manner to reduce the risk of unwanted data loss through data exfiltration. While both CTI and ISMS are widespread in modern cyber security strategies, most often they are implemented concurrently. Our process, however, is based on the hypothesis that the mitigation of data loss is improved if both CTI and ISMS interact with one another and complement each other conclusively. Our concept makes use of the MITRE ATT&CK framework in order to enable (partial) automatic execution of our process chain and to execute proactive simulations to measure the effectiveness of the implemented countermeasures and to identify any security gaps that may exist.

Keywords: Cyber Threat Intelligence · Data Exfiltration · Information Security Management System

1 Introduction

The ubiquitous use of the Internet increases both the quantity and quality of network-based attacks and thus the need for protection against this class of risk. Widespread network-based attacks are attacks against the availability of services (e.g. denial of service attacks in their different variants) and attacks on the

* Supported by organization Bundeswehr University Munich

confidentiality of data, respectively. In this paper we address the second attack class, which is relevant for instance in the scope of espionage, blackmailing, or ransom. More precisely, while many research is published with respect to detection of a network breach, we focus on the detection and prevention of data exfiltration as a major challenge of contemporary network security.

A common category of concepts and measures to protect networks is Cyber Threat Intelligence (CTI). CTI is a way to improve cyber security by an improved assessing of the real existing threats. CTI provides information about the threats to business. CTI thus helps to understand and prioritize the relevance of known and yet unknown future cyber threats for one's own business. Therefore, it is an effective method to strengthen the security of business information systems [39, pp. 1–2].

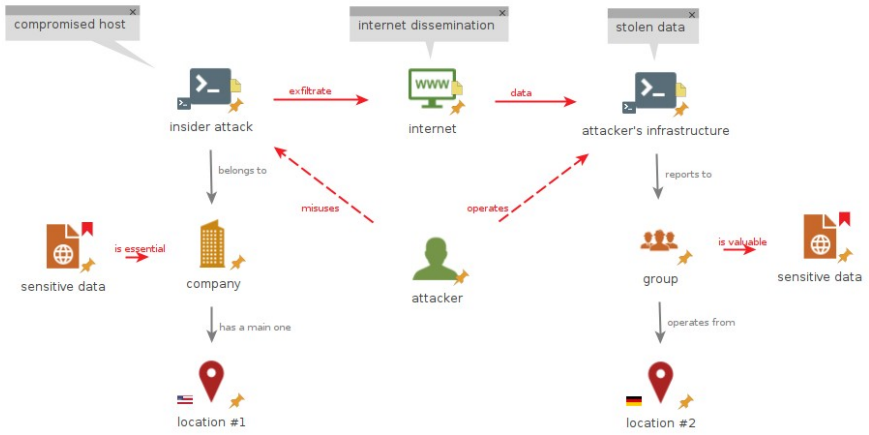

Fig. 1. Use Case Data Exfiltration [33]

We use CTI as a base concept to specifically mitigate the dangers of data exfiltration for the respective business. Our use case and the relevant parties are illustrated in figure 1. As of today methods have been investigated to automatically derive the business context from the currently known vulnerabilities. Formatting and sharing technologies are increasingly used like the Structured Threat Intelligence eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII) [39, p. 1]. Feeds, downloadable in JSON format, are increasingly being implemented to inform in a timely manner.

On the other hand institutions implement their cyber security strategy by releasing an Information Security Management Systems (ISMS). While often CTI and ISMS are implemented loosely coupled in a concurrent way, the goal of our paper is to introduce a concept to reduce the risk of unwanted data loss through data exfiltration in a dynamic manner by combining both CTI and ISMS. Furthermore, we use the MITRE ATT&CK framework to implement and later on automate CTI.

The main purpose of the paper at hand is to describe the connection between the CTI and ISMS processes and thus, building on two proven processes, to achieve added value in favor of reducing the risk of data theft. The Business Process Modulation and Notation is used for this and code examples are given for the implementation of this value-adding approach.

In more detail, our contributions are as follows: First, the essence of CTI [10] is examined in terms of how it can be procedural integrated into an organization and which parameters have to be supplied. Second the basic process for ensuring information safety and security [19, 17] is checked to see whether suitable connecting points to CTI can be identified. After all, it is important to find the right controls [18] in order to effectively link the processes with one another. The ISO 27K series [19] is used as the framework for this work. Third the entire process is formally noted using [1] in order to provide companies with the necessary framework – a Business Process Management System (BPMS) [13] for the future as illustrated in figures 8 and 9. Finally we provide a sample use case based on the "SilverTerrier" group to show how our concept works.

The rest of the paper is organized as follows: in Section 2 we review and systemize the related work in our scope. Then Section 3 presents the concept of Cyber Threat Intelligence followed by Section 4, where we explain our proposal for usage of the MITRE ATT&CK framework to mitigate data exfiltration. Next we introduce Information Security Management Systems in Section 5. Our concept to jointly make use of Cyber Threat Intelligence and Information Security Management Systems is then presented in Section 6.1. We conclude our paper in Section 7 and point to future work.

2 Related work

The work of this paper is going a first step towards bridging the gap between CTI and the current conditions of the enterprise IT-systems by combining CTI and ISMS using the MITRE ATT&CK framework. Respect is given to the current sensitive data on the assets of the enterprise. To the best of our knowledge, there is currently no existing research activity in this specific focus. In this section we present related work in the scope of data exfiltration, especially as part of an Advanced Persistent Threat (APT). Additionally related work with respect to the MITRE ATT&CK framework is discussed.

Scientific research regarding to adversary data exfiltration has a long history. Yet, 2014, the anatomy of typical attacks was examined. Referencing to an article of the Center for the Protection on National Infrastructure (CPNI) it was

stated, that different advanced attackers were using different tactics. Different tactics are used to penetrate IT-systems of enterprises, institutions as well as Industry Control Systems (ICS) in order to identify sensitive, valuable data. Finally, identified sensitive data is exfiltrated by utilizing advanced data transfer hiding technologies [32, pp. 6–7]. The imperative of establishing effective security controls was distinguished [32, pp. 16–32].

Very early, the threat of unauthorized data exfiltration over various channels has been understood [32, pp. 8–12]. Therefore, the range is varying from the simple exploitation of websites, like YouTube (simply uploading Gigabytes of videos) or Timblr, up to complex hex dumping of video frames [37, p. 4].

Until today, research has often been focused on examinations of specific methods. Single exfiltration channels have been investigated in order to figure out effective countermeasures, each. To name some of these data exfiltration methods: Structured Query Language (SQL) attacks against sensitive relational databases [12], cryptography signature based detection [22], detecting DNS over HTTPS [21], exploiting minification of web applications [34], stealthy data exfiltration from Industry Control Systems (ICS) by manipulating Programmable Logical Controllers (PLC) [11], bridging the air gap with audio signaling [30].

Accompanying the rising usage of encryption for storing and transferring data, appropriate techniques have been investigated to track data transmission in spite of encryption. The idea of deep packet inspection is one example for this [20]. The same intention is recognizable regarding the mushrooming implementations of steganography [40]

Multi layer approaches were exploited. In particular, Advanced Persistent Threats (APT) have learned to exploit multiple layers for achieving the diversion of sensitive data in a hidden manner. Interactively, detection capabilities have been researched with this trend [29].

Machine Learning was contemplated with confidence. Multi approaches have been evaluated and reviewed to utilize machine learning in order to reveal multi layer data exfiltration activities [3].

Innovation of information technology went hand in hand with more complex threats. Big data lakes have been born. The number of available data sources as well as the frequency of updating data by the Internet of Things (IoT) have grown significantly. Big data and real-time sensors were brought in. Corresponding, the necessity to examine misuse potential - among others data exfiltration - grew up and is culminating just today. Real time processing and streaming data processing will create new opportunities for big data analytics and will enable rapid threat prediction [25, pp. 58–59].

With the same speed in which the data exfiltration techniques are becoming more complex, defense approaches are enhancing. Geolocation-practice has been discovered today in order to filter valid participants for a data transmission and to prevent unauthorized data exfiltration [21]. Skills and training are advancing to foster the evolution of effective countermeasures; best practices lecture for the utilization of machine learning for cyber security purposes with python may be one example for this [15].

The Markov Belief Model figured out how to predict data exfiltration activities by APT. The model envisaged the likelihood in close correlation to the phase of the adversaries attack. Different phases of phases caused different operational figures. The Markov Belief Model transferred the prediction towards multiple phases of the attack. The likelihood of unauthorized data exfiltration is predicted with respect to each phase of the attack. The closer contemplation of the data exfiltration process itself was begun by Markov [14].

Different approaches have been reviewed. On the one hand, different levels are contemplated: strategic, operational, tactical level. Threat modeling is done at every level. On the other hand, Asset-Threat-Data-System concentric threat modeling approaches are pursued [23, pp. 3–4]. Information sharing becomes more important; MITRE provides for example the ATT&CK in the Structured Threat Information Expression (STIX) JSON format via Github [23, p. 14]. The future will bring further approaches in order to overcome the limits of today. So far, APT are not understood completely nor a bit detected in a timely manner. The future may require a more effective process. The process may have to consume the TTPs as well as historical and current data of attack vectors. Furthermore, current vulnerabilities in an enterprise IT have to be considered. With respect to the knowledge on current sensitive data of organizations assets, future trend processes will have to combine all the factors more holistically [23, pp. 14–15].

3 Cyber Threat Intelligence

Cyber security and forensics experts have to detect, analyze and defend against cyber threats in almost real-time. A timely response to cyber attacks is required. Without a deeper understanding of cyber attacks, effective countermeasures are hardly possible. The thought of limiting the threats makes threat intelligence gaining more importance. For this purpose, data mining techniques are being further developed in a targeted manner [10, p. 1]. A significant amount of data from security monitoring solutions and reports has to be transformed into knowledge. CTI is assigned this task.

The CTI model, which we use in our work, is depicted in figure 2. Indicators for the detection of cyber attacks are determined. The information about cyber attacks is systematically evaluated. Cyber criminals try to steal sensitive data. An attack follows a life cycle. It starts with spying on the target. Unfortunately, it often ends with criminal acts on the victim's IT system [10, p. 2].

Now it is particularly important to find the point of attack and uncover the vulnerabilities before cybercriminals exploit them. Points of attack are already extremely diverse today: non-traceable communication, 0day vulnerabilities, malicious PDF documents are just a few examples. The previous approaches show gaps. In addition, cybercriminals are increasingly using dangerous antiforensic and evasion disruptive measures. Other known disruptive measures require more modern approaches to forensic examination of exchanged and stored data. In the recent past, numerous countermeasures have been tried including artificial intel-

ligence's machine learning [10, p. 3]. CTI is now focusing on the evaluation of cyber attack methods [10, p. 4].

The goals are improved detection and then improved responsiveness. A current awareness of the cyber threat situation is the basis. The companies have now reached a certain level of maturity. Data is recorded systematically. The exchange of data speeds up the process. Known threats are prioritized from the company's perspective. The implementation of security controls is being driven forward in a targeted manner. In order to collect high quality data, an ontology is required. This ontology must be as comprehensive as possible. A model serves this purpose. The model is the semantic representation of the cyber threats. It offers the possibility to standardize metrics. The model provides the basis for deriving quantitative metrics [24, pp. 1–2].

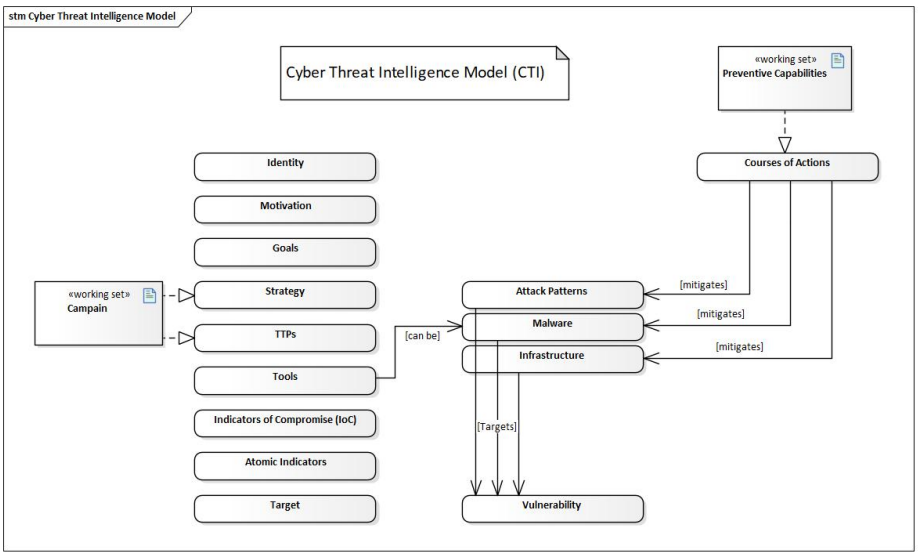

Fig. 2. Reference Architecture: Cyber Threat Intelligence Model [24, p. 2]

Diverse taxonomies have already developed. Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Characteristics (CAPEC) are two examples. The MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework also offers usable insights into the entire life cycle of the attack, including the preparatory and follow-up phases. Finally STIX is the most used for sharing structured threat information.

The interrelationships as illustrated in Figure 2 are fundamentally used as a model for CTI. In addition, the model is already being used today to build up knowledge bases, which in turn can then be systematically queried as required [24, p. 6]. In the case of the CTI model, the starting points for mitigating the threats are of particular interest here.

4 MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) is a globally accessible knowledge base [27]. It provides a common taxonomy for CTI. It is about telemetry sensing and behavioral analytics. The ATT&CK model covers multiple technology domains: Enterprise, Mobile, Industry Control Systems (ICS). The model is a concrete instance and implementation of the abstract CTI model in figure 2. It provides a mitigation object structure, too.

Mitigations represent security concepts and technologies in the ATT&CK framework. These represented technologies help to prevent a technique or sub-technique being executed successfully. These mitigations are described vendor-agnosticly. The ATT&CK Mitigation Model comprises the attributes Name, ID, Description, Version and Techniques addressed by mitigation.

The MITRE ATT&CK object model relationship is illustrated in figure 3. Its high-level components, like mitigation, are in relation one with the other. These are Adversary Groups, Technique / Sub-Technique, Software, Tactic and Mitigation. Each component is described with such an object structure, hence structures and relationships to describe adversaries' behavior are recorded in these object structures systematically. Figure 3 is showing the fundamental relationships of the objects [27] as well as an concrete sample of a manifestation of these objects regarding to a group named APT 39.

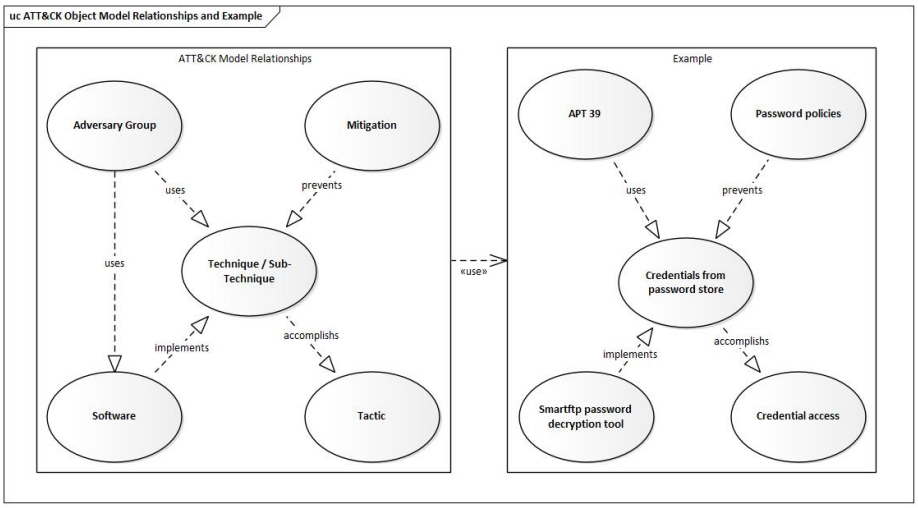

Fig. 3. ATT&CK Object Model Relationships and example [27]

The ATT&CK Object Model implements the abstract layer of the Cyber Intelligence Model which is shown in figure 2. The TTPs were taken over directly, the Adversary Group entity of the MITRE ATT&CK framework corresponds to

the identity of the CTI Model. The software component corresponds to the tools, etc [27]. The data is continuously recorded within the MITRE ATT&CK framework on the basis of publicly accessible analysis reports of cyber analysts for current attacks. Therefore, current threat data is continuously managed within the MITRE ATT&CK framework.

In order to mitigate the risk of an attack, it is first of all necessary to understand possible techniques that can be used. The data now describes the known techniques and how they are used, along with aids for their detection and mitigation. The recommended measures relate to the attack technique currently under consideration [36, p. 1]. The standardization of the CTI is undertaken in order to be better informed about the cyber risks. The awareness of the situation becomes even better if this data is exchanged with other people at risk and affected. Effective cooperation arises. More analytics are now used to find hidden vulnerabilities and to make decisions about mitigating the threat posed by them [31, p. 310].

The MITRE ATT&CK Navigator offers a simple user interface to navigate through the MITRE CTI databases and to annotate facts [28]. We present a snapshot of it for the tactic 'Exfiltration' in Figure 4. In its current version all domains are supported. These are Enterprise, Mobile, Industry Control Systems (ICS). In order to consider CTI for IT networks of organizations or companies, enterprise and possibly mobile are the right entry points.

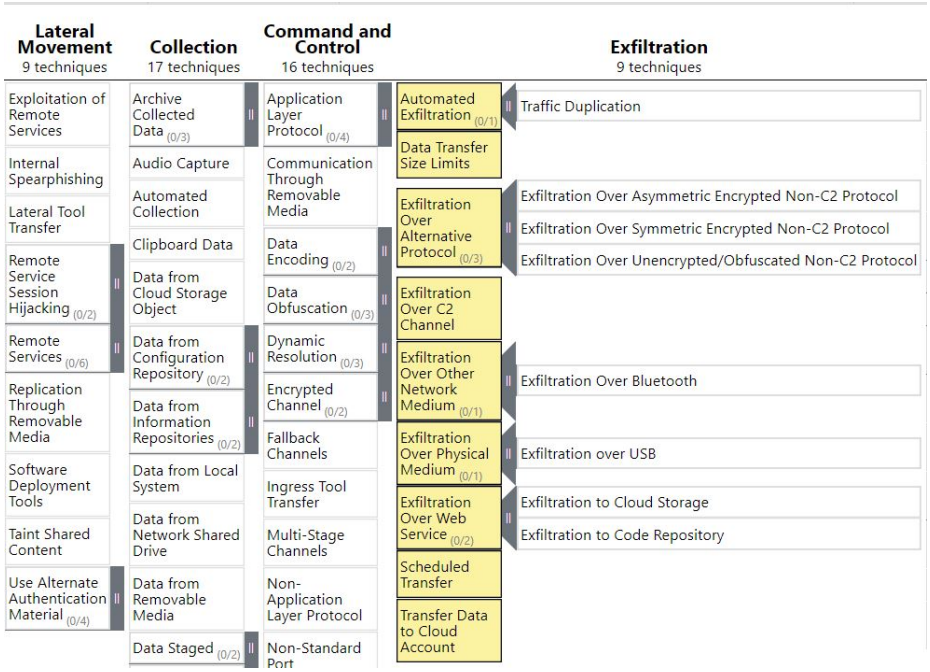

Fig. 4. ATT&CK Navigator Enterprise, Tactic 'Exfiltration' [28]

If an incident that has become known is evaluated, the applied techniques (including sub-techniques) are selected in the matrix of the MITRE ATT&CK Navigator and so the complete attack procedure is revealed. Conversely, the attack procedures of known groups can be selected from the CTI database in order to find out about their Tactics and Techniques [27]. One of the Tactics led is exfiltration.

In the course of CTI, conclusions can be drawn about the techniques and subtechniques used by known groups for exfiltration of sensitive information. If, in addition, the adversarial techniques used exploit weak points that also exist in your own company, then the focus can be identified in this way, at which the measures to mitigate the risk are currently to be located.

This process is then partially automated so that the necessary human interaction is concentrated on essential decisions. Therefore, the MITRE corporation maintains a GitHub repository [26]. Also Python libraries like [2] [5] are applicable for transactional access to the data. The interfaces are standardized via STIX encoded in Java Script Object Notation (JSON) and the TAXII application protocol to transfer CTI via the Hypertext Transfer Protocol Secure (HTTPS) between participants [7]. The Python classes abstract the access to the interfaces and offer constructs for the direct evaluation of the data. The following Listing 1.1 shows the code block for loading of all currently available data sets regarding threats to enterprises into the processing memory. The loaded data can then be evaluated using differentiable filter methods so that, among other things, the mitigation measures with regard to current threats of data theft can be extracted.

```
import requests
from stix2 import MemoryStore

def get_data_from_branch(domain, branch="master"):
    """get the ATT&CK STIX data from MITRE/CTI. Domain should be 'enterprise-attack', 'mobile-attack' or 'ics-attack'. Branch should typically be master."""
    stix_json = requests.get(f"https://raw.githubusercontent.com/mitre/cti/{branch}/{domain}/{domain}.json").json()
    return MemoryStore(stix_data=stix_json["objects"])

src = get_data_from_branch("enterprise-attack")
```

Listing 1.1. Access CTI via stix2 Python API [5]

Listing 1.2 is utilizing the Python "technique_mappings_to_csv.py" from the MITRE ATT&CK scripts [7] in order to extract mitigation measures against currently used exfiltration techniques. The results are written into a comma separated values file which is then easily visualized e.g. in a data mining application as shown exemplary in figure 5. This approach opens up the possibility of further automation. Above all, the open, documented interfaces enable efficient querying of the available CTI databases. Targeted queries allow an ever better focus on measures to mitigate the currently prevailing threats of data theft.

```
python3 technique_mappings_to_csv.py -d ''enterprise-attack''
    -m mitigations -t exfiltration -s Current.csv
```

Listing 1.2. Querying and filtering MITRE CTI database

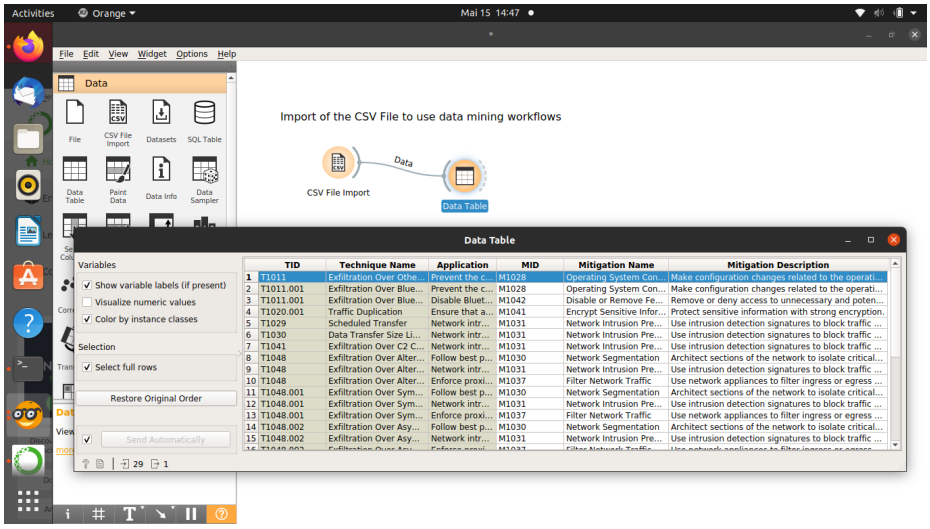

Fig. 5. Manual Data Mining with the results of CTI [16]

5 Information Security Management Systems

ISO/IEC 27000:2018 provides an overview of Information Security Management Systems (ISMS). Essential terms are defined. An attack is described with the attempt to destroy, uncover, change, disable, steal, gain unauthorized access to a value and use it without authorization [19, p. 7]. The relationship between stealing and data exfiltration is obvious. Furthermore, information is identified as a value that requires adequate protection of availability, confidentiality and integrity [19, p. 20]. Here it is the protection of confidentiality that is called into question by data exfiltration. It also states that appropriate measures are defined, implemented, monitored and, if necessary, improved so that the specific information security and business objectives of the organization are achieved. These measures can be seamlessly integrated into the business processes of the organization [19, p. 22].

It is precisely this question of the seamless integration of measures to mitigate the risk of data theft that must now be considered further. How can the measures to mitigate the risk of data theft be integrated into the ISMS? It must

Table 1. ISO actions for continuous improvement of the ISMS

ISO	Action
a)	Analyzing and evaluating the existing situation to identify areas
b)	Establishing the objectives
c)	Searching for possible solutions to achieve the objectives
d)	Evaluating these solutions and making a selection
e)	Implementing the selected solution
f)	Measuring, verifying, analyzing and evaluating results to determine that the objectives have been met
g)	Formalizing changes

also be ensured that any risk assessment is carried out methodically and is suitable for producing comparable and reproducible results [19, p. 25]. All actions necessary to bring about an improvement are listed in sequential order as listed in table 1. These mandatory actions for improvement, as these are listed in the ISO norm [19, p. 17], are repeated cyclically.

The nature of cyber security in practice is that it is not so obvious whether a decision may cause risk and damage [4, p. 1]. So, there is the need for a process. In order to run substantial business successfully, you have to get systematic about cyber security quickly. In today's networked systems, risks aggregate, cascade effects arise, inter-dependencies lead to accumulation of risks. It is essential to introduce systematic ways of identifying these risks [4, pp. 2–3]. Regular processes must be introduced or existing ones supplemented. In order to find the right entry point here, the basic processes of the company are first considered.

ISO 27001:2013 describes the requirements for an ISMS. Good planning is credited with preventing or at least reducing undesirable effects and achieving continuous improvement [17, p. 8]. It is written that it is imperative to determine the methods of monitoring, measurement, analysis and evaluation. In addition, the time and frequency of the inspection must be specified [17, p. 14]. These requirements will be carried over to mitigation measures. The objectives and corresponding procedures are listed in table 2 and offer some interesting starting points for mitigating unwanted data exfiltration. The ISO 27002:2013 [18] then provides instructions for implementation of each procedure. The information from both documents is compiled here.

6 Concept and Example to integrate CTI with ISMS

Looking at our hypothesis to link the two areas of CTI and ISMS using the MITRE ATT&CK framework to mitigate the threat of unwanted data exfiltration, all components have been introduced. In this section we turn to the details of the connection of CTI and ISMS. We first explain our concept in Section 6.1 and then apply it in Section 6.2 to a sample use case.

Table 2. Categories of measures [17] [18]

Identifier/Type	Description
A.8.1.1	**Inventory for values**
Procedure	Information and other values of the company are recorded, an inventory is drawn up and maintained
Measures	determine values, document importance, manage lifecycle (creation-processing-storage-transfer-deletion-destruction), designation of those responsible, compilation of an inventory list of values
A.8.2.1	**Classification of information**
Procedure	Information is classified based on legal requirements, its value, its criticality and its sensitivity to unauthorized disclosure
Measures	classify information considering confidentiality, use a uniform scheme relating to data exfiltration (safe-slightly-significant, short-term effects, serious impact on strategic goals)
A.12.6.1	**Handling of technical vulnerabilities**
Procedure	Information about technical weak points is obtained in good time. The hazard is assessed. Appropriate measures are taken to address the risk
Measures	Define tasks and responsibilities, identify data sources, define a time schedule for the reaction, assess risks, determine remedies, execute remedies, test patches, regular review and evaluation of the process, coordinate with incident response process, defining the actions in the situation without the possibility of mitigating the risk
A.14.3.1	**Protection of test data**
Procedure	Test data is carefully selected, protected and controlled
Measures	Avoid the use of Personally Identifiable Information (PII) or other sensitive test data, obtain authorization from the person in charge, delete test data, log, use of test data that is as similar as possible to the operating data
A.18.2.1	**Independent review of information security**
Procedure	The organization's approach to handling information security and its implementation are reviewed independently at regular intervals or whenever there are significant changes
Measures	Appoint an independent auditor, check at regular intervals or if there are significant changes, consider corrective action

6.1 Concept to integrate CTI with ISMS

In this section we describe and show our concept to integrate CTI with ISMS. We make use of BPMN diagrams to explain our concept. BPMN diagrams in general offer a standardized form of notation in order to implement our proposed procedure across departments in the organization. The two diagrams showing our concept are depicted in Figure 8 and Figure 9, respectively.

First of all, Figure 8 shows our Communication Diagram from the pool of BPMN diagrams. The communication relationships between relevant actors of the CTI and the ISMS are shown. Leading actors as explained in table 3 are involved on behalf of the areas of the organization. The cyber analyst is working on being aware of the current cyber threats. He pays special attention to the dangers of data theft. The CISO receives regulated knowledge of the current situation of threats to the organization. The cyber analyst reports to him. At the same time, the cyber analyst communicates the current threats to the information security officer. This information is used to target the activities of the ISMS. The Information Security Officer reports to the CISO on the current status of the ISMS. If necessary, possibilities for improvement are communicated with the CISO and suggested for implementation. CISO evaluates the status of CTI and ISMS and controls as required. After all, the CISO is responsible for the completeness and effectiveness of the ISMS vis-à-vis independent auditors. For this purpose, the relevant parameters are communicated and the results of the audit are received. The diagram shows these communication relationships and assigns the communication relationships to the actions in table 1 and measures from table 2. CTI and ISMS are linked to one another via the selected measures and found suitable actions of the ISO standard 27K. In this way, the ISO actions that are often already known and used can continue to be used with added value. The ISO standard is very often the basis for certification. If such a certification exists, it will not be affected by our solution and hence constitutes a decisive advantage of our proposed process.

Table 3. Leading actors

Actor	Description
CISO	Chief Information Security Officer. Control of the ISMS, here in particular the actions for continuous improvement.
Indipendent Auditor	Independent authority to review the existence and effectiveness of the ISMS processes
Cyber Analyst	Selected and specially trained staff to develop current awareness of cyber threats
Information Security Officer	Employees to carry out the sub-processes and actions of the ISMS in the day-to-day operation of the company

In our second BPMN diagram shown in Figure 9, the integration of CTI and ISMS is viewed from a further perspective. This time, an activity diagram is used. The activities of the actors are arranged in so-called swim lanes. In this way, the actions are assigned to the actors. Responsibilities and the process become visible. Figure 9 shows how the findings of the CTI are used specifically in the ISMS. In the event of a later automation, the identified, current threats to data theft or their mitigation measures are extracted and transferred as a configuration file. This configuration controls the need to select appropriate test data from the company. The rules, specified by the ISO for handling test data, are used here. The test data correspond as closely as possible to the sensitive data that are currently threatened. Permission to use these test data must be obtained in each case (ISO A.14.3.1). Finally, the configuration file of the CTI is used in turn to align the preventive protective measures. In line with the current threat situation, network protocols (e.g. DNS Query, HTTPS Replace Certificate, ICMP, BGP Open) and communication methods (e.g. DNS over TLS, Drop Box LSP) for simulating the attack are now being set appropriately. The simulation is now carried out focused on this configuration. Vulnerabilities to current threats become apparent. These vulnerabilities are quickly worked out into opportunities for improvement. The test data will then be deleted. Proposals for improvement that have been approved for implementation are formally incorporated into the documentation.

The entire process chain is repeated cyclically. The frequency is necessarily derived from the security ambitions of the organization. This concept of jointly making use of CTI and ISMS integrates resources gently into the organization and potentially quickly mitigates the risk of data theft. Through the preventive approach, the initiative against cyber attackers is regained. Through the use of organization-specific test data and the simulation on the IT system actually to be protected, concrete opportunities for improvement are highlighted that can be implemented immediately.

6.2 Example to apply our concept

The international cyber reporting shows more and more references to the activities of the "SilverTerrier" group. The SilverTerrier group is attributed to Nigeria and is known to target high technology companies [6]. The CTI of your institution is getting aware of the situation and is starting the procedure of our concept.

The MITRE ATT&CK framework is first exploited. The context shown in Figure 3 is used to first determine which options are available to this group. The malware "Agent Tesla" is assigned to this adversary group. This malicious code is assigned the area of application via the ATT&CK framework to execute the "Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol", Figure 6, technique [8].

This technique is described in the framework as follows: Sensitive data is encoded and compressed with publicy available algorithms and then exfiltrated using protocols like HTTP, FTP and DNS. The constant data traffic on these

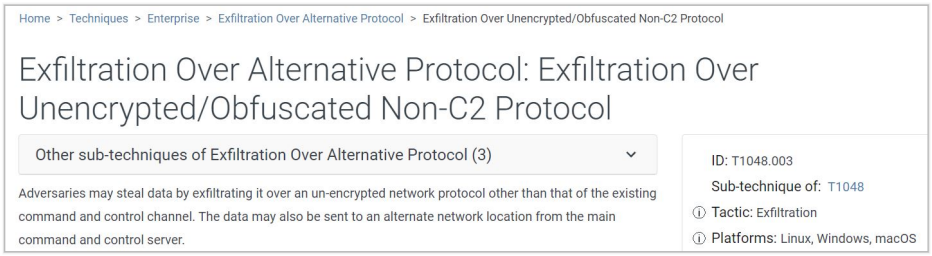

Fig. 6. MITRE ATT&CK Framework identified technique [9]

channels obscures the data exfiltration or at least makes it difficult to identify this adversary activity [9].

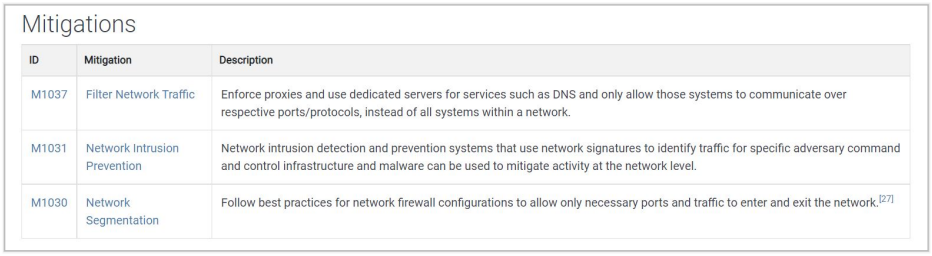

Fig. 7. MITRE ATT&CK Framework Mitigations [9]

The MITRE ATT&CK framework also shows mitigation measures in Figure 7. By comparing these mitigation measures with the existing security measures of the ISMS, it can be determined immediately whether adequate measures are already being used to mitigate this risk. With reference to the communication diagram in Figure 8, this is the first coordination between the cyber analyst and the information security officer. Both roles are described in table 3.

The further course of action is now configured based on the identified threat situation. Appropriate test data from the organization is carefully selected in reference to the ISO security controls A.8.1.1, A.8.2.1 and A.14.3.1 in table 2. The effectiveness of the countermeasures is specifically checked against this particular risk of data theft now. This is done by simulating this step for the domestic IT system as shown in Figure 9. With reference to the current hazard, the protocols, e.g. HTTP, ICMP, DNS [9] are now deployed for the purpose of simulation. In this paper we propose our conclusive process, the data extraction methods have to be implemented and evaluated in a later phase of our work. If applicable, existing open source projects can help as the first code basis. The following list shows examples of some of the methods to do this:

– HTTP(S)

- ICMP
- DNS
- SMTP/IMAP
- Raw TCP

The simulation of the threat is executed as pointed out in Figure 9. Technical vulnerabilities may become apparent in the process. Through the simulation, traffic data is reflected in the log files of the monitoring systems. In the extreme case, the simulated attack penetrates the protection of the organization. In any case, traces will remain which can later be evaluated and used to reinforce mitigation measures. Vulnerabilities are fed back into the regular ISMS and processed using the ISO 27002 A12.6.1 catalog of measures as referenced in table 2. In addition, help is given by the MITRE ATT&CK framework on how the technique can be detected. Here are these suggestions for the example:

- Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server)
- Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious
- Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.

Identified vulnerabilities and the recommendations to detect the specific risk are now included in the management of the vulnerabilities as input variables. They are evaluated in the context of the ISMS process for continuous improvement against the security goals of the organization and then implemented (Figure 9). With this approach, the regular process for continuous improvement of the ISMS is proactively served with the results of the simulation. One anticipates the current danger and strengthens the protective measures before – here in this example – the group "SilverTerrier" [6] can successfully achieve the data theft.

Concretely, options to improve your own protective measures can be derived. For example, based on the results and logfiles of the simulation training data sets for machine learning or deterministic measures such as extended firewall rules can be created profitably. Because the results of the simulation are included in the ISMS process (Figure 9), which is managed directly by the CISO (Figure 8), the decision-making authority is given to make direct and immediate decisions for the organization. In this case, the mitigation measures against the current technique [9] are implemented or improved. In this way, the critical improvement can be introduced in a timely manner against the current threat of the APT [6].

7 Conclusion

In this paper we investigated the procedural link between CTI and ISMS in relation to the mitigation of data exfiltration using the MITRE ATT&CK framework. We derived and explained a formally noted process, which offers suitable

support for implementation and proves the hypothesis of our concept. Fundamental measures for the passive protection of the IT system regarding unwanted data outflows were not in the current scope of our work, a reference is made to other papers [35] in this regard.

In future work we will implement and evaluate the proposed CTI process. We will create a software code base to identify the current threats via CTI in order to initiate the simulation of the most common relevant attacks. Existing protective measures are checked in a targeted manner, gaps are uncovered and the actual threat is counteracted preventively. The long-term goal is then the implementation of the simulation engine and the design of extensive test series for the final manifestation of the described combined CTI-ISMS process.

References

[1] Object Management Group (OMG). *Business Process Model and Notation*. 2021. URL: https://www.bpmn.org/ (visited on 04/27/2021).

[2] Organization for the Advancement of Structured Information Standards (OASIS). *OASIS TC Open Repository: Python APIs for STIX 2*. 2020. URL: https://github.com/oasis-open/cti-python-stix2 (visited on 05/10/2021).

[3] Barbar M.Ali Bushra Sabir Ullah Faheem and Raj Gaire. "Machine Learning for Detecting Data Exfiltration: A Review". In: *Computer Science* (2020).

[4] Fred Cohen. *Bad decision-making OR Making bad decisions*. 2021. URL: http://all.net/ (visited on 05/05/2021).

[5] OASIS Cyber Threat Intelligence Technical Committee. *STIX 2 Python API Documentation*. 2021. URL: https://stix2.readthedocs.io/en/latest/ (visited on 05/10/2021).

[6] MITRE Cooperation. *MITRE ATT&CK Group Silver Terrier*. 2021. URL: https://attack.mitre.org/groups/G0083/ (visited on 05/31/2021).

[7] MITRE Cooperation. *MITRE ATT&CK Scripts*. 2021. URL: https://github.com/mitre-attack/attack-scripts/tree/master/scripts (visited on 05/15/2021).

[8] MITRE Cooperation. *MITRE ATT&CK Software Agent Tesla*. 2021. URL: https://attack.mitre.org/software/S0331/ (visited on 05/31/2021).

[9] MITRE Cooperation. *MITRE ATT&CK Technique Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol*. 2021. URL: https://attack.mitre.org/techniques/T1048/003/ (visited on 05/31/2021).

[10] Conti Mauro Dargahi Tooska and Dehghantanha Ali. *Cyber threat intelligence*. 978-3-319-73950-2. Cham Springer, 2018.

[11] Anastasis Keliris Dimitrios Tychalas and Michail Maniatakos. "LED Alert: Supply Chain Threats for Stealthy Data Exfiltration in Industrial Control Systems". In: *2019 IEEE 25th International Symposium on On-Line*

Testing and Robust System Design (IOLTS) On-Line Testing and Robust System Design (IOLTS) (2019).

[12] Gabriel Ghinita Elisa Bertino. "Towards mechanisms for detection and prevention of data exfiltration by insiders: keynote talk paper". In: *ASIACCS 11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (2011). URL: https://dl.acm.org/doi/10.1145/1966913.1966916.

[13] Harald Kühn Franz Bayer. *Prozessmanagement für Experten, Impulse für aktuelle und wiederkehrende Themen*. ISBN 978-3-642-36994-0. Springer Verlag, 2013.

[14] P. Louvieris G. Ioannou and G.Powel. "A Markov multi-phase transferable belief model: An application for predicting data exfiltration APTs". In: *Proceedings of the 16th International Conference on Information Fusion Information Fusion (FUSION)* (2013).

[15] Soma Halder and Sinan Ozdemir. *Hands-On Machine Learning for Cybersecurity : Safeguard Your System by Making Your Machines Intelligent Using the Python Ecosystem*. 9781788992282. 9781788990967. Birmingham, UK : Packt Publishing, 2018.

[16] Anaconda Inc. *Anaconda - Data Science technology for human sensemaking*. 2021. URL: https://www.anaconda.com/ (visited on 04/01/2021).

[17] International Electronical Commission (IEC) International Standard Organization (ISO). *Information Security Management*. 2013. URL: https://www.iso.org/isoiec-27001-information-security.html (visited on 04/30/2021).

[18] International Electronical Commission (IEC) International Standard Organization (ISO). *Information technology — Security techniques — Code of practice for information security controls*. 2013. URL: https://www.iso.org/isoiec-27001-information-security.html (visited on 04/30/2021).

[19] International Electronical Commission (IEC) International Standard Organization (ISO). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. 2018. URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip (visited on 04/30/2021).

[20] Raluca Ada Popa Justine Sherry Chang Lan and Sylvia Ratnasamy. "Blind-Box: Deep Packet Inspection over Encrypted Traffic". In: *SIGCOMM '15: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication* (2015). URL: https://dl.acm.org/doi/10.1145/2785956.2787502.

[21] L. Jean Camp Kevin Benton. "Firewalling Scenic Routes: Preventing Data Exfiltration via Political and Geographic Routing Policies". In: *SafeConfig '16: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense* (2016). URL: https://dl.acm.org/doi/10.1145/2994475.2994477.

[22] Archibald Rennie Liu Yali Corbett Cherita, Mukherjee Biswanath, and Ghosal Muhherjee. "Detecting sensitive data exfiltration by an insider attack". In: *CSIIRW '08: Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead* (2008). URL: https://dl.acm.org/doi/10.1145/1413140.1413159.

[23] Sami Azam Matt Tatam Bharanidharan Shanmugam and Krishnan Kannoorpatti. "A review of threat modelling approaches for APT-style attacks". In: *Heliyon* (2021). URL: https://www.cell.com/heliyon/fulltext/S2405-8440(21)00074-8.

[24] Bromander Siri Mavroeidis Vasileios. *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*. 2021. URL: https://www.duo.uio.no/bitstream/handle/10852/58492/CTI_Mavroeidis.pdf?sequence=4 (visited on 05/02/2021).

[25] Natialia Miloslavskaya. "Stream Data Analytics for Network Attacks Prediction". In: *Procedia Computer Science 2020 169:57-62* (2020). URL: https://www.sciencedirect.com/science/article/pii/S1877050920302374.

[26] MITRE. *ATT&CK Version 9.0. The Cyber Threat Intelligence Repository of MITRE ATTCK and CAPED catalogs expressed in STIX 2.0 JSON*. 2021. URL: https://github.com/mitre/cti (visited on 05/10/2021).

[27] MITRE. *MITRE ATT&CK Framework*. 2021. URL: https://attack.mitre.org/ (visited on 03/30/2021).

[28] MITRE. *MITRE ATT&CK NAVIGATOR*. 2021. URL: https://mitre-attack.github.io/attack-navigator/ (visited on 03/30/2021).

[29] Ali Hadi Mohammad Ahmad Abu Allawi and Arafat Awajan. "MLDED: Multi-Layer Data Exfiltration Detection System". In: *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic* (2015).

[30] Andrey Daidakulov Mordechai Guri Yosef Solewicz and Yuvai Elovici. "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers". In: *Computer Science* (2016).

[31] Brad Hibbert Morey J. Haber. *Asset Attack Vectors : Building Effective Vulnerability Management Strategies to Protect Organizations*. ISBN 9781484236260. Berkeley, CA : Apress. 2018, 2018.

[32] MWR InfoSecurity (Head Office). "Detecting and Deterring Data Exfiltration - Guide for Implementers". In: *Centre for the Protection of National Infrastructure* (2014). URL: https://www.researchgate.net/profile/Mohamed_Mourad_Lafifi/post/Any_good_ICS_Dataset_contains_exfiltration_data_leakages/attachment/5be5a43fcfe4a7645500ee64/AS%3A691074662141959%401541776447655/download/Detecting-Deterring-Data-Exfiltration-Guide-for-Implementers-.pdf.

[33] Maltego organization. *Website Maltego*. 2021. URL: https://www.maltego.com/ (visited on 04/20/2021).

[34] Pawel Rajba and Wojciech Mazurczyk. "Exploiting minification for data hiding purposes". In: *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security* (2020). URL: https://dl.acm.org/doi/10.1145/3407023.3409209.

[35] Travis Ashley Roger Kwon and Nikhil Sri. "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping". In: *2020 Resilience Week (RWS) Resilience Week (RWS), 2020. :106-112 Oct, 2020* (2020).

[36] Marc Ruef. "Monitoring-Detecting Attacks with MITRE ATT&CK". In: *scip Labs, Zenodo* (2019).

[37] Stefano Braghin Spiros Antonatos. "4Kdump: Exfiltrating files via hexdump and video capture". In: *CS2 '19: Proceedings of the Sixth Workshop on Cryptography and Security in Computing Systems* (2019). URL: https://dl.acm.org/doi/10.1145/3304080.3304081.

[38] Sparx Systems. *Website Sparx Systems - Enterprise Architect*. 2021. URL: https://www.sparxsystems.de/ (visited on 04/21/2021).

[39] He Ying Xu Yuanchen Yang Yingjie. "A Representation of Business Oriented Cyber Threat Intelligence and the Objects Assembly". In: *IEEE 10th International Conference on Information Science and Technology (ICIST) Information Science and Technology (ICIST)* (2020). URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7795373.

[40] Sam Yoon. "Steganography in the Modern Attack Landscape". In: *Carbon Black* (Apr. 9, 2019). URL: https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/.

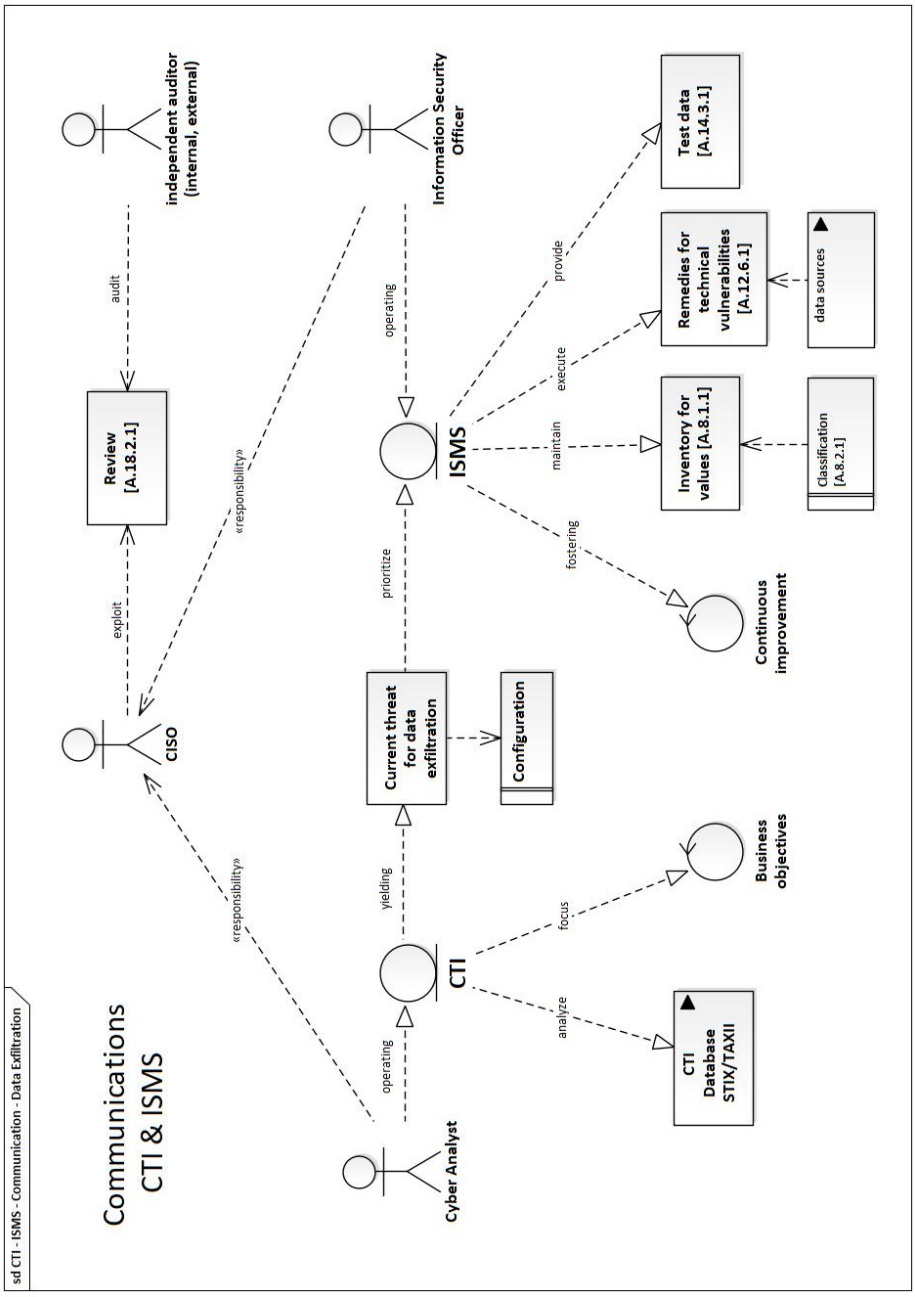

Fig. 8. BPMN - Diagram Communications for CTI & ISMS [38]

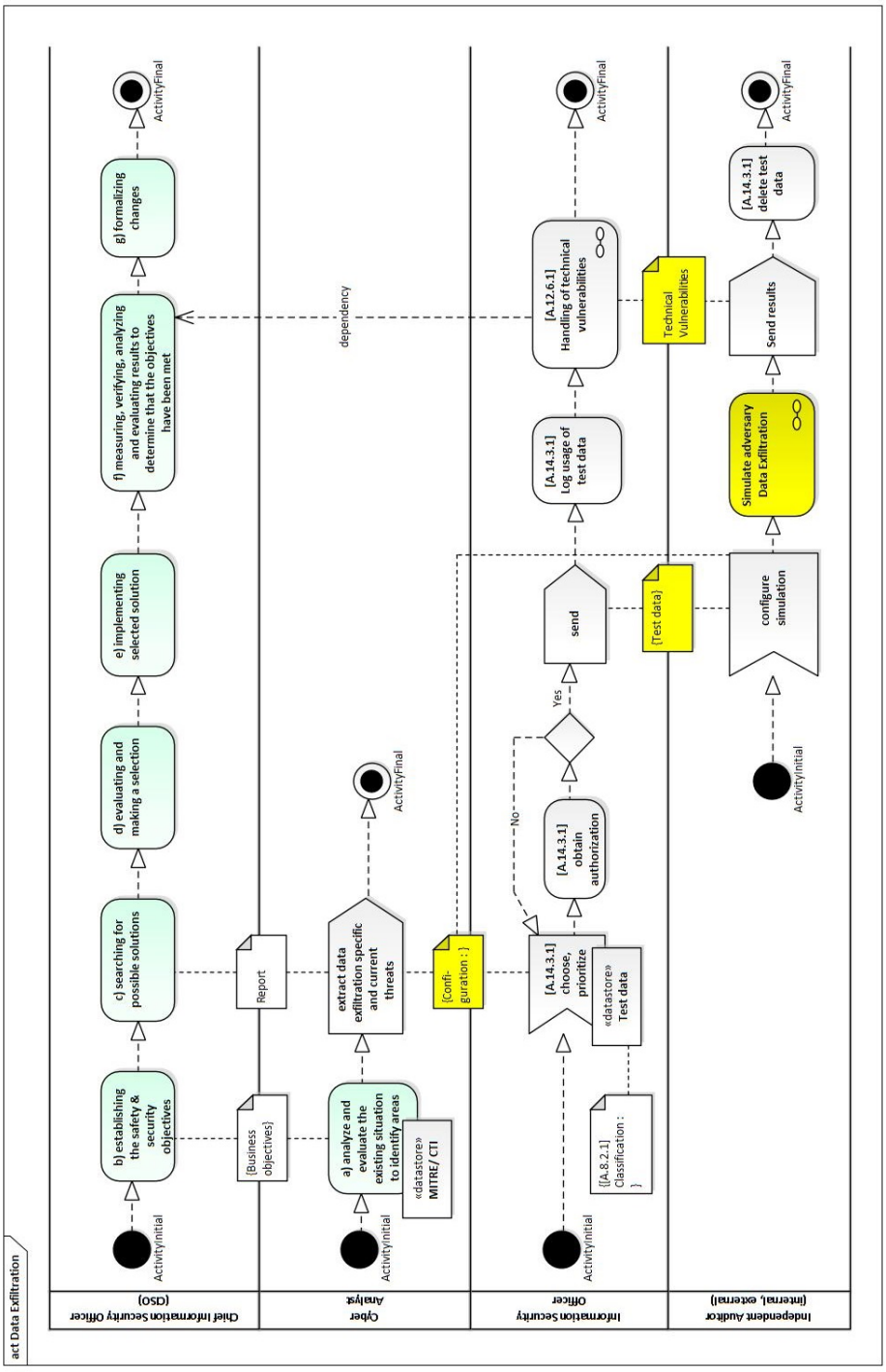

Fig. 9. BPMN - Diagram Activities for CTI & ISMS relating data exfiltration [38]