Enhancing Incident Management by an Improved Understanding of Data Exfiltration: Definition, Evaluation, Review

Michael Mundt[1(✉)] and Harald Baier[2]

[1] Esri Deutschland GmbH, Bonn, Germany
m.mundt@esri.de
[2] Research Institute CODE, University of the Bundeswehr Munich, Munich, Germany
harald.baier@unibw.de
https://www.esri.de, https://www.unibw.de/digfor

Abstract. Whether it is an insider or an Advanced Persistent Threat (APT), sensitive data is being stolen. This year's German Federal Office for Information Security (BSI) annual report (https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html) on the state of Information Technology's (IT) Security in Germany points to the worsening situation. A key result of the BSI is that cyber extortion attempts have become the number-one threat due to leading cyber-attacker collectives expanding their strategy. They exfiltrate data unlawfully for offsite storage before encrypting it. This year, the organizations were also being extorted for hush money and faced with the threat of disclosure of sensitive, but stolen data. Data exfiltration has become a standard procedure in almost all cases of ransomware attacks. In our work, we take up this currently most dangerous threat. First, we provide a universal definition for the operation of data exfiltration. In the next step we evaluate three frequently used methods for cyber threat intelligence: Microsoft Threat Modeling Tool, the Malware Information and Sharing Platform (MISP), and the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework. Our evaluation goal is to find out whether these methods allow to investigate and describe data exfiltration in an appropriate way. In particular, we search for a suitable categorization structure and semantics in order to categorize data exfiltration approaches. Given this, we carry out a systematic research, where we consider recent peer-reviewed publications from the *Digital Threats: Research and Practice (DTRAP)* forum in the context of data exfiltration. We categorize data exfiltration techniques as they are described in the papers. This provides an excellent indication of the focus and distribution and allows us to specifically address deficiencies and further research needs related to data exfiltration categories. Finally, we identify and choose one relevant example of a category of data exfiltration and show interactions with detection and protection measures. Our work provides an excellent assessment of the subject matter, frequently used tools

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 570, pp. 33–57, 2024.
https://doi.org/10.1007/978-3-031-56580-9_3

and current research priorities in the context of the threat of adversarial data exfiltration.

Keywords: Advanced Persistent Threat · Data Exfiltration · Universal Definition · Cyber Threat Intelligence · Systematic Review

1 Introduction

Network-based attacks and their mitigation are of increasing importance in our ever-connected world. Often network-based attacks address valuable data, which the attacker either encrypts to extort ransom or steals to make money reselling, or both. After the infamous WannaCry and NotPetya ransomware attacks in 2017, companies stepped up their cyber defenses. More emphasis was placed on backup and recovery processes so that even when files were destroyed, organizations had copies for quick recovery. However, cyber criminals have also adapted their methods. Instead of simply encrypting files, double or even multiple extortion [59] ransomware now exfiltrates the data first, before encrypting it. In particular, valuable business assets must be checked for unauthorized access and need to be protected [56]. This year's Federal Office for Information Security (BSI) annual report[1] on the state of Information Technology's (IT) Security in Germany confirms that cyber extortion attempts have become the number-one threat due to leading cyber-attacker collectives, who expand their strategy.

As a key element of incident management institutions often implement their cyber security strategy by releasing an Information Security Management Systems (ISMS). This approach provides robust protection against fundamental threats from cyber-attackers. Institutions are increasingly focusing on holistic protection of their own IT and are activating professional defense mechanisms such as Extended Detection and Response (XDR). It is about the consideration of an overall process. First of all, as far as possible, all data sources are used. The goal is seamless monitoring of the data sources. Incoming data is analyzed immediately with the aim of initiating coordinated defense processes. In addition, XDR approaches pursue the goal of continuously optimizing these autonomous security processes. Knowledge of the threats posed by cyber-attackers is constantly increasing. The technical, legal and procedural possibilities for sharing information about cyber threats are constantly improving. Experts are emerging who are specifically addressing these cyber threats and making their skills available to others as a service.

However, such protection mechanisms are often considered late and sometimes only after a successful cyber-attack. Companies' livelihoods fail when their intellectual property is stolen. Often, modern protection measures are being adapted too hesitantly. In addition, cyber-attackers have also become more professional and specialized. Very sophisticated techniques for data exfiltration, such

[1] https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

as steganography, are increasingly being used. Professionals develop these technologies and offer them as a service to other criminals. As a result the BSI recommendation for incident management of data exfiltration (and presumable subsequent disclosure of data) is a recommendation for a systematic and rule-based approach to monitor data transfers. That is the way to identify unusually large outbound flows of data and terminates them in good time.

Definition and Review. We provide an universal definition of data exfiltration. Thus, we manifest an initial anchor point. We start from this content anchor point and review existing literature. Then, at its core, this work involves a systematic literature review. Our goal is to find out what methods and techniques for hostile extraction of data have been scientifically studied in the period 2020–2022. We attempt to list the variety of methods and techniques and evaluate what skills are needed by an attacker in order to use them and hence - in the scope of incident management - to defend them. The result is an initial evaluation matrix.

Evaluation. We explore three frequently used frameworks. Here, we select the Microsoft Threat Modeling Tool[2], the Malware Information Sharing Platform (MISP)[3], and the MITRE ATT&CK framework[4]. First, we review the level of detail in which data exfiltration can be structured and described using each of these methods. With a view to the categorization to be conducted later, we select one method which fits best for our purpose to describe threats of data exfiltration in categories structurally and semantically. The selection criteria are the maturity, the simplicity of application and finally the international recognition. Based on this, we assign all the methods and techniques studied in the given categories. Through this we gain knowledge, on the one hand about known attack-vectors and on the other hand about techniques for data exfiltration. Furthermore, we figure out the current focus of the considered scientific community in this way.

Structure of the Paper. The rest of this paper is structured as follows: after the short motivation in this introduction we turn to related work in Sect. 2. In Sect. 3 we provide our definition of data exfiltration and evaluate the before-named frameworks. Next Sect. 4 contains our systematic review and the categorization. One chosen sample case study follows in Sect. 5. Finally we conclude our paper in Sect. 6 and point to future work.

2 Related Work

In this section we sketch related work to our three contributions, i.e. the definition of *data exfiltration*, the evaluation of the three frequently used CTI frameworks, and the systematic review in order to categorize techniques for data exfiltration.

[2] https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool.
[3] https://www.misp-project.org/.
[4] https://attack.mitre.org/.

With respect to the definition of data exfiltration, in many works initial approaches to provide a taxonomy for data exfiltration are considered. Overviews and summerizations are available (e.g., [22]). However, to the best of our knowledge, we have not found an "ex pressis verbis" universally applicable definition in the large body of literature. In our work, we now provide this.

A small number of papers is available which describes the cyber threat intelligence tools and techniques evaluated in our work. However, for us it is a matter of describing the tools through mapping the specific use case of data exfiltration. Nevertheless, here is a sample work for the Microsoft Threat Modeling Tool [63] and the MITRE ATT&CK framework [1]. Such work was also carried out for the MISP. This example shows an approach for modeling a threat model for Infrastructure as a Service (IaaS) offerings [62]. Further studies, each focused on individual areas of application, are available, e.g., [66]. We could not identify any work that specifically examines these applications in order to determine whether it is possible to describe and to categorize the phenomenon of data exfiltration in sufficient detail with a common and internationally used taxonomy. Our investigation fills this gap. We decide on the most appropriate categorization for data exfiltration techniques.

[68] provide an excellent overview and review of state-of-the-art data exfiltration publications and aspects. As attacker type their review distinguishes between an outside party or an insider. Furthermore [68] discriminate between network-based and physical data exfiltration. Both attack-categories are further subdivided: sample network-based data exfiltration comprise direct download, passive monitoring, phishing, while physical theft and dumpster diving are assigned to physical data exfiltration. Additionally, [68] consider countermeasures. However, this review is already 4 years old and no comparably extensive works have been published since then. Our work now examines the most recent publications from this year and thus does justice to the rapid technical innovations that are (unfortunately) also used by cyber criminals.

There is a great deal of work on investigating specific threats or attacks through a concrete technique of data exfiltration. This is an example of how Internet of Things protocols are exploited to leak data [69]. Very often, these works are focused on a specific vulnerability. We choose a different approach. Starting from a selected category for data exfiltration, we explain the interrelationships in order to improve protective measures. The level of abstraction is higher - category instead of individual vulnerability - and offers companies the possibility to analyze the threat more holistically.

3 Definition, Evaluation of Methods, Categorization

In this Sect. 3.1 we first provide a short definition of the term *data exfiltration* followed by our evaluation of frequently used CTI frameworks with respect to the targeted categorization of data exfiltration in Sect. 3.2. Finally Sect. 3.3 provides insights into the before-chosen categorization schema.

3.1 Definition

According to the current German Federal Office for Information Security (BSI) annual report[5] cyber extortion attempts have become the number-one threat. Typically cyber extortion is based on data exfiltration, which addresses the fundamental security objective *confidentiality*. Our definition is thus as follows:

Data exfiltration describes a breach of the security goal of confidentiality. It leads to disclosure of data to an unauthorized party (e.g., an attacker, an intruder) typically by transferring the data over a public network. The disclosed data may be either stored or otherwise processed in an IT system or transmitted over a network.

Further notes for the threat are given by the General Data Protection Regulation (GDPR) [19, Art. 4 (12)]. Therein is described that 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. It becomes clear that data breach is a subset of data exfiltration following our definition.

3.2 Evaluation of Frequently Used Frameworks

In the sequel, we evaluate three frameworks on their suitability to categorize the threat of data exfiltration. We are looking for an internationally recognized and easy to understand method that we will later apply to the researched papers. In addition, we use these findings (preliminary study) in future work.

Microsoft Threat Modeling Tool. Microsoft Threat Modelling Tool is a simple software application. Templates for threats and elements are included. The purpose of the tool is to support a secure software development process [50]. The underlying concept provides user functionality to design software architectures, which are then examined for threats in the course of the cyclic software development process. Identified threats are eliminated or suitably mitigated at the earliest possible stage in the software development cycle [28]. The threat analysis is based on the STRIDE model [51]. This categorizes different types of threats. One of the categories is *Information Disclosure*. We understand this as an abstraction of data exfiltration. The tool provides the functionality to create data flow diagrams. Here, so-called elements are connected with each other, and the data flow direction is displayed. In addition, there is the possibility of editing trust areas. Simple examples of these are IT-segments in a company, demilitarized zones or the public internet. Figure 1 is showing a simple sample of such a dataflow diagram.

Moreover, the tool offers the possibility to freely model the threats according to your own ideas. Templates are provided. We look at the Information disclosure threat in a supplied threat modeling template for Azure Cloud Services.

[5] https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lageberichte/lagebericht_node.html.

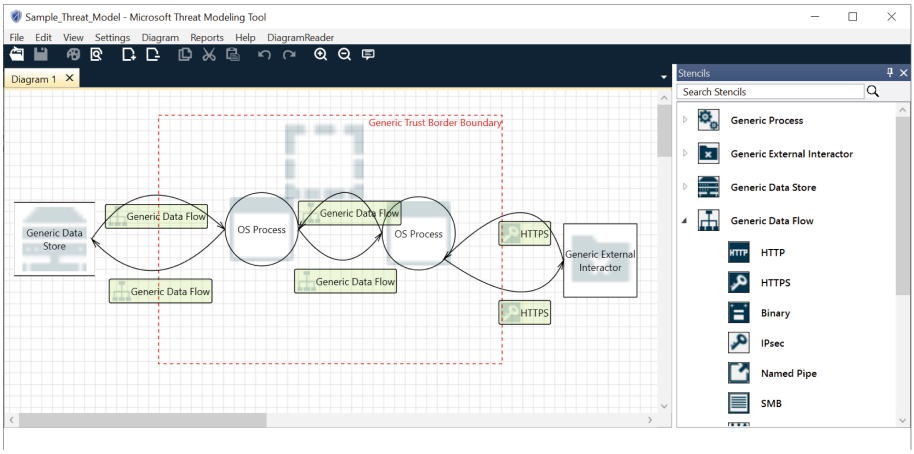

Fig. 1. Dataflow diagram built with Microsoft Threat Modeling Tool

The template has numerous entries for the Information Disclosure category e.g.: an adversary may read content stored in {target.Name} instances through SQL injection-based attacks, an adversary may gain access to sensitive data from log files, [...] and to unmasked sensitive data such as credit card numbers. The concept is to adjust these entries according to the individual situation. The entries do not have the character of a generally valid, internationally agreed categorization. The STRIDE threat model is very abstract. Basically, the STRIDE threat model combines the threat of information disclosure with the security objective of confidentiality. The further detailing of the threat is to be done individually and depending on the individual situation in the currently considered software development lifecycle.

The tool now offers the functionality to assign the threats to the individual elements via the data flow diagram. Each of the elements (processes, data stores, data flows, and interactors) has a set of threats it is susceptible to [28]. Doing so, the diagram provides information on the paths in which the entire system can fail. Threats and their interactions become more visible. A team of experts can now for example focus on analyzing the threats of unintentional data leakage. Data flows, data stores and process are potentially susceptible to the threat Information Disclosure. In the context of data exfiltration, particular attention is paid to elements of these groups. The Microsoft Threat Modeling Tool supports analysis with functionality. The reporting tool automatically identifies all data flows at trust zone transitions so that mitigation actions have to be identified and discussed.

In our opinion, this tool is very well suited, for example, to create an initial overview of the software's architecture and discuss it in an architecture review board. We see the tool as a possible tool among others of the ecosystem such as Static Code Analysis and Security Testing Tools. We also consider regular penetration tests at least for all major releases to be expedient.

MITRE ATT&CK Framework. This is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The advanced persistent threats (APT) activities described are derived from publicly available reports of known incidents. These sources are used: Threat intelligence reports, conference presentations, webinars, social media, blogs, open-source code repositories, malware samples. Research results are also included that reveal procedures with which frequently used protective measures can be undermined. Cyber analysts around the world are working on this [13, p. 21]. The framework consists of an entry web page [13] with interactive access to different matrices, a Cyber Threat Intelligence (CTI) repository [12] in Structured Threat Information eXpression (STIX) format, several companion documents [15–17], and an interactive application with basic functions for navigating, searching, tagging, and storing based on the information repository [14]. The framework provides a common taxonomy for structuring and describing Tactics, Techniques and Procedures (TTP). Tactics [16, p. 8] are the intentions of an attacker. The implemented concept is based on the assumption that an attack is a sequence of Tactics. Exfiltration is one of these tactics in the nomenclature of the framework.

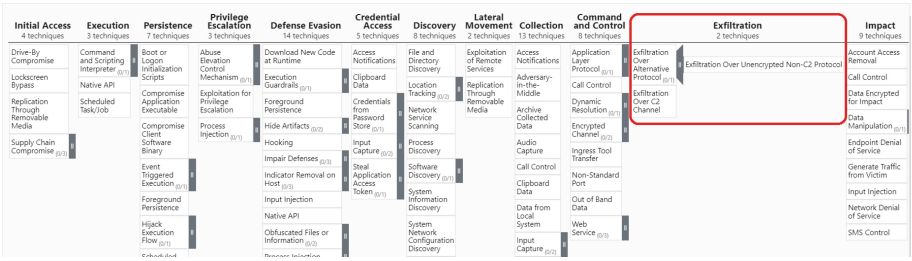

Fig. 2. Tactic Exfiltration within Mobile Matrix

Techniques now describe, how the attacker is achieving a Tactic by performing an action. Specific implementations of a certain Techniques - procedures - are attributively documented as procedure examples for a given Technique [16, pp. 9–12]. Other objects such as APT-Groups, Software, Data Sources and Mitigations supplement the information model in the latest version 12.1, the Campaign object has been added. All objects are logically related to each other [16, pp. 17–18]. The entry is made via matrices. Matrices are available for different domains: Enterprise, Industry Control Systems (ICS), Mobile. Each matrix is spanned horizontally by the successive Tactics and vertically by the associated Techniques [16, pp. 6–7]. We use the Navigator application to browse the matrices. In the Mobile domain, for example, Tactic Exfiltration has two Techniques (see Fig. 2). A Sub-Technique is assigned to one of them. We will show the further details of the "Scheduled Transfer"[6] Technique. This Technique is used for data exfiltration. First of all, the Technique is described in general. Metadata

[6] https://attack.mitre.org/techniques/T1029/.

like the date of creation and the last update, the version and a unique identification number are noted. Furthermore, several procedure examples, mitigation measures, detection capabilities, and the sources for all of this information are captured. The available human interfaces as well as the Python library [33] and the REST interfaces [12] for exchanging data in the STIX format are used to access the repository data and use it analytically for the purpose of CTI.

The taxonomy is in use internationally and proves to be simple and understandable enough to be learned and applied by cyber analysts worldwide. The common taxonomy is complex enough to include the aspects of the Technique in sufficient detail. Specific implementations for technical protection measures, which may be product-specific, are not included. The focus is clearly on CTI.

MISP. This is an open-source threat intelligence and sharing platform. The MISP Core Software [70] facilitates exchange and sharing of threat information as well as Indicators of Compromise (IoC) about targeted malware and campaings [11].

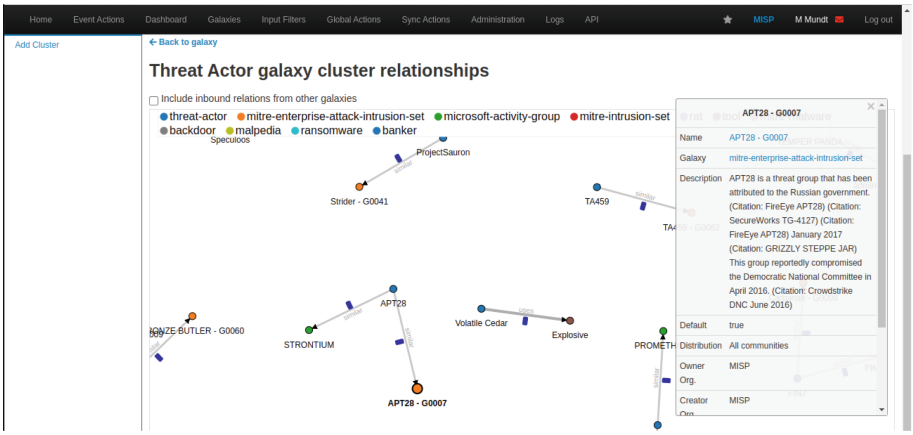

Fig. 3. MISP Galaxy and Connection Graph

The introductory website [32] provides comprehensive documentation on functionality, on handling of the software and on the inside-used information models. An open REST interface allows data exchange in STIX format. A Python library is available [33]. The object model is generic. The smallest unit is a building block. Such a building block is containing a piece of information (attribute) to be shared like an IP-address or a file hash. The next higher level of the object model is called MISP object. These are compositions of attributes. Events are another simple but specialized building block containing formatted text messages. Object references are the binding link. They create relationships between the building blocks. In this way, they can be used to represent a connection graph whose nodes consist of the building blocks and edges of the object references (see

Fig. 3). A correlation engine is integrated. Whenever a new attribute is created or an existing one is modified, the engine checks and establishes correlations with respect to the existing Object references and events.

The software offers the functionality to set tags. Tags are used for further marking and description. There are free tags, which the user can fill with free text as desired. This simplest form of free tag offers maximum flexibility for the individual user, but often also leads to disadvantages.

```
{
  "description": "ATT&CK Tactic",
  "icon": "map",
  "kill_chain_order": {
    "mitre-attack": [
      "reconnaissance",
      "resource-development",
      "initial-access",
      [...]
      "discovery",
      "lateral-movement",
      "collection",
      "command-and-control",
      "exfiltration",
      "impact"
    ],
        .....
```

Listing 1.1. GitHub repository of a MISP taxonomy

They make collaboration difficult and may even prevent the sharing of information with common understanding. Not everyone may be able to understand the free text tags. To avoid this disadvantage there are Taxonomies and Galaxies in the MISP project. Taxonomies and Galaxies are exchanged internationally with the aim of achieving internationally accepted semantics. Taxonomies are simple label standards and common sets of vocabularies which serve well because of their ease of consumption and automation. A taxonomy for data exfiltration does not exist at the time of our investigation. The Listing 1.1 shows the taxonomy for MITRE ATT&CK Tactics[7]. Each taxonomy is continued in a GitHub project in the JSON notation. Simple tags and its presentation are standardized in this way. In our assessment, taxonomies are not currently suitable for providing an appropriate categorization of data exfiltration methods. Their composition is too simple. Galaxies and Galaxy Clusters are advanced set of vocabularies containing metadata. Galaxies enable MISP users to describe more complex high-level information. The cyber kill chain of the attack is such a context. Internally, galaxies are used to represent the MITRE ATT&CK framework. We consider the example from before, the Technique Scheduled Transfer

[7] https://github.com/MISP/misp-galaxy/blob/main/galaxies/mitre-attack-pattern.json.

of the MITRE ATT&CK framework. This is modeled in a MISP Galaxy[8]. In the Galaxy the description is taken over as well as the identification number. In addition, a return link to the corresponding technique of the MITRE ATT&CK framework is included. From now, a tag (see Listing 1.2) is used in the MISP software to express the context. Corresponding building blocks are labeled with this tag.

```
misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029"
```

Listing 1.2. MISP galaxy for Exfiltration-Technique Scheduled Transfer

Thus, even the MISP project uses the MITRE ATT&CK framework to model the context of the attack vector and thus the Techniques with the objective of data exfiltration. The construct of MISP Galaxies is used to represent the individual objects in form of a tag. The core software also offers the functionality to automate workflows. This is of particular importance when information needs to be processed in real time and human interaction is too slow. Here, the individual events can be conditionally linked to each other by means of a graphical interface. The resulting chain is then executed automatically as soon as the initial event occurs. In addition, the software already imports a wealth of feeds[9] in the default configuration in order to directly integrate current information on incidents, which can then in turn be quickly correlated or compared with each other.

In our assessment, the purpose of the MISP software is the quick identification and modeling of current malware and its usage in current campaings. MISP is also about sharing individual malware information in realtime. For this purpose, data sources are integrated. A high degree of automation is achieved. The MISP correlation engine tempts to cluster in an automatic manner. Workflows for collaboration and sharing are implemented.

Assessment. In conclusion, we want to present the final assessment of our evaluation in form of an overview in Table 1. The frameworks studied serve different purposes. Use cases for each are well-known in the community. The level of abstraction for adversary techniques is the decicive distinction between them. This results in different application focuses and also the different need for processing speed. Internationally recognized are all three, so this criterion does not provide us with a distinguishing aid here. The question of the level of detail and the consistency of the structure and semantics will be the decisive factor. For our later application purpose, the individual techniques for data exfiltration must be able to be categorized conclusively and the schema used for this must not be subject to rapid and individual changes. In our view, these criteria enable a resilient categorization schema.

[8] https://www.misp-project.org/galaxy.html#_scheduled_transfer_t1029.
[9] https://www.misp-project.org/feeds/.

Table 1. Selection Criteria

Framework	Level of Abstraction	Processing Speed	Main Purpose
Microsoft Threat Modeling Tool	High	Duration of the driven Secure Software Development Lifecycle	Implementation of the Principle Security by Design in Software Development
MITRE ATT&CK framework	Mid	Released app. Twice a year	Internationally used taxonomy and data repository in the context of Advanced Persistent Threats cyber-attack-vectors
MISP Platform	Low-/Mid-	Close real time processing	Analyze current attacks and domains and share insights on current malware campaigns within MISP community

The following assessment matrix (Table 2) indicates with [+] a positive and with [−] a negative assessment for using each framework for the purpose of this work. The Microsoft Threat Modeling Tool is providing a high level of abstraction. In the case of data exfiltration only the umbrella term of "Information Disclosure" is offered. This does not give us the opportunity to categorize the data exfiltration techniques later. The selection criteria is evaluated negatively. The lifetime of the information depends in each case on the passage of a software development cycle. Here we need a more constant categorization, which is independent of indivduellen time divisions. The life time here is not too high from the change speed but we need a period more independent of individual processes. The Mitre Attack Framework identifies Tactic Exfiltration and sorts under it nine categories of different techniques for data exfiltration. In addition, there is a single technique in the ICS matrix in the Tactic "Impact" that is used to steal data. This is excellent for our task and we evaluate it positively.

Table 2. Assessment

Framework	Level of Abstraction	Processing Speed	Internationally Standardized	Total
Microsoft Threat Modeling Tool	[−]	[−]	[+]	[−]
MITRE ATT&CK framework	[+]	[+]	[+]	[+]
MISP Platform	[−]	[−]	[+]	[−]

The framework is updated about twice a year. The structure can also be changed in the process. For example, new techniques for data exfiltration can be

added if they are described in cyber incident reports. We consider this consistency to be sufficient. In any case, our categorization would have to be adjusted when new Techniques appear in the MITRE ATT&CK framework and we use the given Techniques for our categorization. The important point here is that this needs to be monitored to ensure comparability with later work. MISP provides the functionality to describe occurring IOC in deep detail and to correlate (automatically) with other indicators. This is about the detection of individual malware. The correlation happens in real time as well as changes to it. This functionality is not very suitable for a long-term comparable categorization. Both properties are considered negative for our application purpose.

The *MITRE ATT&CK framework* turned out to be the right framework for the task of categorizing upcoming techniques for data exfiltration on the tour of our systematic literature research. We will utilize the Techniques for categorization[10]. The Sub-Technics are not considered. We consider the Techniques to be sufficient for the intended purpose and we want to keep it as simple as possible for later comparability.

3.3 Categorization Based on the MITRE ATT&CK Framework

The MITRE ATT&CK framework lists the following Techniques used to achieve the goal of data exfiltration (see Table 3). Each of these Techniques is assigned a unique Identity (ID). These Techniques are umbrella terms for the procedures used, which are further subdivided in a variety of ways. Obviously, data exfiltration can be executed in various ways. Starting with simple means, e.g., copy-pasting files onto an external device or cloud, to more sophisticated, obfuscating exploitation of IT network protocols. Once the data has been exfiltrated from the attacked IT system, there is no longer any realistic possibility to ensure the confidentiality of this data.

4 Systematic Literature Recherche

We conduct systematic research of the publications of a modern forum. We have evaluated the journal DTRAP. DTRAP is a peer-reviewed Gold Open Access journal that targets the prevention, identification, mitigation, and elimination of digital threats. DTRAP aims to bridge the gap between academic research and industry practice[11]. As such, the journal is ideally suited to examine current developments applied in practice in the context of data exfiltration. At the beginning, we queried all publications of the past year of the journal. For this we have used the query which you may see in Listing 1.3.

The search yields a result list of fifty-three publications. The search is conducted on 30th December 2022. All results have passed the peer review process. Some work dates back to the period 1999–2021. All publications considered are

[10] https://attack.mitre.org/tactics/TA0010/.
[11] https://dl.acm.org/journal/dtrap.

Table 3. Categorization by MITRE ATT&CK framework [52]

ID	Exfiltration Technique	Description
T1020	Automated Exfiltration	Use of automated processing for gathered sensitive data
T1030	Data transfer size limits	To circumvent a transfer size limit the whole data is split in fixed size chunks
T1048	Exfiltration over alternative protocols	Misusing standardized IT network protocols
T1041	Exfiltration over a command and control (C2) channel	Misusing the main communication channel of the attacker
T1011	Exfiltration over Network Medium	Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel
T1052	Exfiltration over physical medium	Misusing removable drives like Universal Serial Bus (USB), cellular phone, MPEG-1 Audio Layer (MP) 3, processing devices
T1567	Exfiltration over web service	Exploiting a legitimate external web service often permitted by firewalls
T1029	Scheduled transfer	Performed at certain times or within specific time intervals
T1537	Transfer data to cloud account	Transferring data including backups to the attacker's cloud account

in 2022. We sift through the list of results and identify the data exfiltration procedures and technologies under investigation in each publication. Four entries of the result list refer to conferences with content in the context of our query.

```
Search: [All: "data exfiltration"] AND [All: techniques] AND [E-
    Publication Date: (01/01/2022 TO 12/31/2022)]
```

Listing 1.3. Querying DTRAP journal

Here we focus on the actual publications. The headings of the conferences are not considered further. This is for example the case for ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security[12]. Whenever possible, we assign the method of data exfiltration under study in the previously mentioned categories (see Table 3) of the MITRE ATT&CK framework and total the number of investigations each. If assignment to one of the categories is not possible, we identify the method separately and examine whether the introduction of an additional category is recommended. Multiple assignment is possible if several different Techniques for data exfiltration are considered in one publication. Work that generally addresses the risk of data exfiltration has been assigned to the Technique T1020 & Automated Exfiltration that makes use

[12] https://dl.acm.org/doi/10.1145/3538969.

Table 4. Concept Matrix

ID	References	Counts	Keywords
T1020	[3,4,7–9,36–39,43,44,48,53,72–74]	16	Ransomware Attacks, Threat Intelligence Platforms, critical medical infrastructures, SCADA & IIoT in subsea systems, provenance graph, monitor system events in real time, reviews the security challenges in IoT networks, provenance tracking, data provenance for host based intrusion detection systems, disrupt an individual's experience of a home, Principal Component Analysis, enhancing data center security utilizes attack graphs to predict all possible cyber-attacks, cross-host attacker activity correlation, tracking algorithm uncovering causal connections between alerts and propagating priorities, promoting trust and situation awareness for human and artificial intelligence cooperation
T1030	[31]	1	forensic log reduction techniques
T1048	[21,35,41,45,46,55,57,61,71]	9	Simulation, DNS, DNS Encryption, TLS certificate pinning, DNS over TLS and HTTPS, off-label DNS misuse, authoritative DNS measurement studying the large-scale epidemiology of the malware ecosystem, Network Time Protocol (NTP) and the Precision Time Protocol (PTP) as carrier for covert channels
T1041	[6,58,60]	3	comprehensive analysis of the key building blocks of ransomware, taxonomy for Identity Management Attacks, outsourcing matching procedures (e.g., YARA rules) to the hardware
T1011	[2,5,10,23,42,54,65,67]	8	Deep Learning for APT Detection, template-based labeling rules, cyber security reasoning, IoT network data, vulnerabilities of Android platform in Auto and Automotive platform, LoRa analysis, communication, security, and its enabled applications, protecting against event sensor faults and sophisticated attackers in a smart home
T1052	[6,24,29,47,64]	5	Audio Signal, personal and sensitive medical data, data-driven network intrusion detection, asymmetrical power states forcing SRAM state retention across power cycles, Denial-of-Wallet (DoW) attack to serverless tenants
T1567	[25–27]	3	HTML violations, key acquisition and covert transmission method, offensive strategy exploiting steganography
T1029	[40]	1	open-source supply chain attacks
T1537	[18,43]	2	Ransomware Attacks, identity and access control in hybrid cloud infrastructure

of automated processing for gathered sensitive data. The assignments and totals are shown in a concept matrix. The concept matrix provides information on the focus with which the threats of data exfiltration were executed in the past year and potentially reveals gaps in the semantics, to describe them, used. Additionally, a keyword is also noted for each publication. In the sum of all keywords a first impression about the content is created in Table 4.

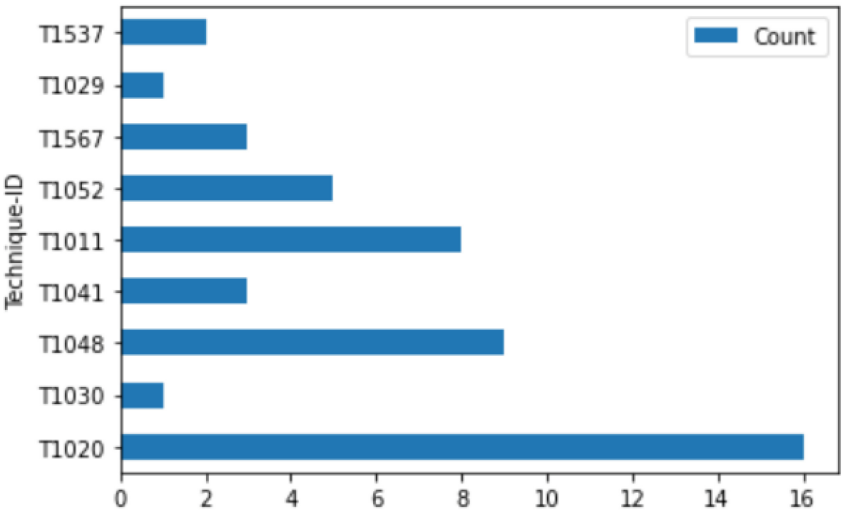

Fig. 4. Simple graphic of the results

One publication of the result list is a comparison of different ransomware attacks. The publication is comparing pre- and mid-pandemic ransomware attacks [43]. Data exfiltration is named as a method of a modern ransomware attacks but not analyzed in detail. One publication is discussing current limitations of threat intelligence platforms leveraging OSINT and a Cyber Threat Unified Taxonomy. Also, in this publication [48], data exfiltration is respected as a method but not investigated in further detail. In another publication [65], points were established and evaluated to help decision-makers understand the significance of cyber threats and to introduce a metric for assessing them. The threat of data exfiltration is included here in a rather general way. All identified methods for data exfiltration could be assigned to the categories of the MITRE ATT&CK framework. The given categories cover the range of the examined method in the research period. We therefore do not recommend an additional, new category. Rather, the selection made is confirmed. The assignment of the examined publications to the categories of methods for data exfiltration is shown graphically in Fig. 4. It is noticeable that two methods appear only once each in a publication during the period under review. These are: **T1030** - Data transfer

size limits and **T1029** - Scheduled transfer. In our opinion, it is these details that need to be taken into account in order to implement effective detection and protection measures. There is certainly a need for further investigation here.

5 Case Study of a Selected Category

We present the advantage of using the MITRE ATT&CK framework categorization in the sequel. We show the Techniques to intent "Exfiltration" in Table 3. The structure of the framework continues to branch until a valuable detail is reached. Each Technique potentially splits into n-further Sub-Techniques. Figure 5 is showing the Sub-Techniques. If an attacker uses such a sub-technique, this leaves digital traces. In the given semantics, these traces are reflected in Data Sources. This relationship is shown in Fig. 6. The content is reduced in favor of a clearer presentation. The data sources splice up into data components. Each data component is accompanied by a description of how it is monitored. We explain these relationships with an example. The Technique T1537 is assigned to the Tactic "Exfiltration": Transfer Data to Cloud Account[13]. This Technique is associated with Data Sources: Cloud Storage, Network Traffic, Snapshot. Each of these Data Sources is in turn related to Data Components e.g., Cloud Storage: Cloud Storage Creation, Cloud Storage Metadata, Cloud Storage Modification.

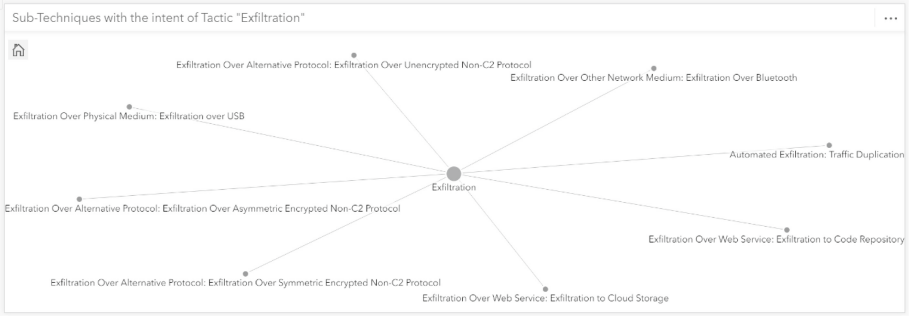

Fig. 5. Sub-Techniques for Exfiltration

Again, each data component is assigned a description of how it can be detected in principle e.g., Cloud Storage Creation: "Monitor account activity for attempts to create and share data, such as snapshots or backups, with untrusted or unusual accounts". In addition, the MITRE organization provides solutions for some of the descriptions in the form of pseudocode or procedures for specific products (see Listing 1.4). This is the purpose of the Cyber Analytics Repository (CAR)[14]. Figure 7 shows these interrelationships. Today, products and services

[13] https://attack.mitre.org/techniques/T1537/.
[14] https://car.mitre.org/analytics/.

are offered to manage a holistic situation picture of all monitored data components in real time. Some of them are already highly specialized for the detection of certain Techniques used to achieve exfiltration [20]. Figure 8 shows once again the interrelations between Data Components and the Technique, for which the Data Components help to detect. For the sake of clarity, the interrelationships are reduced and simplified in the Figure. Rules are offered for widely used cyber security products that can be used directly for detection. Listing for example is showing a rule for a Logpoint Detection and Response product. Thus, the techniques are described in a detail that offers starting points for the implementation of protection measures.

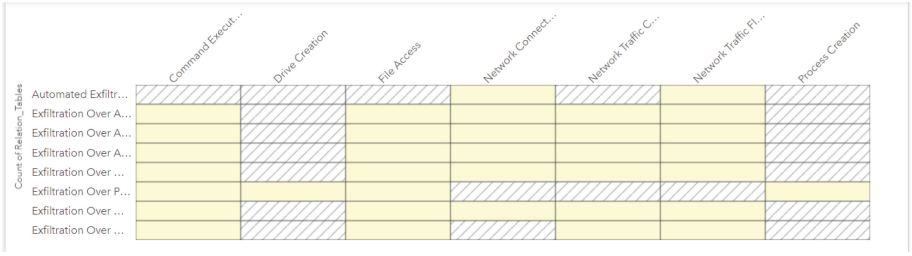

Fig. 6. Data Sources assigned to Sub-Techniques

In addition, the attack vectors can be used to create a checklist and list all data components. This makes it possible to measure and verify the completeness of the protection mechanisms.

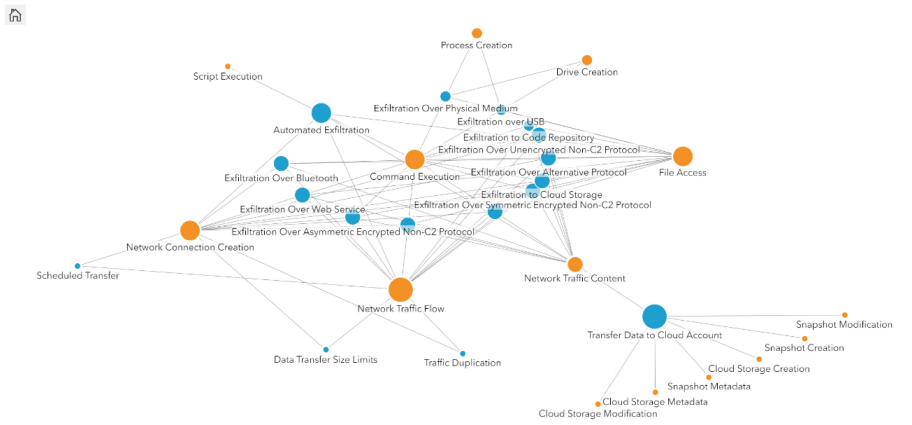

Fig. 7. Data Components detecting Sub-Techniques

Cyber defenders receive valuable checklists to verify the completeness of their efforts. It is now up to the knowledge, experience and skill of the cyber defender to implement the protective measures in an appropriate manner. In addition, knowledge of one's system's data flows opens the way to modern concepts for dynamically segmenting data flows, protecting them in a targeted manner, and sustainably preventing potential cyber-attacks from viewing and assembling sensitive, valuable data in preparation for data exfiltration. Suitable services and software tools [30] are available for this purpose. Last year, the International Organization for Standardization (ISO) and International Electronical Commission (IEC) updated the standard: ISO/IEC 27001:2022 [34]. One of the innovations is the mandatory introduction of the Control requirements for threat intelligence: A.5.7 Threat intelligence. The issue of integrating the Control A.5.7 into the holistic Information Security Management System (ISMS) has been considered in an earlier paper from our workgroup [49]. It can serve as an approach for integrating the "Threat Intelligence" control into the existing control landscape of the enterprise in an effective manner.

```
Example: CAR-2013-10-002
Name: DLL Injection via Load Library
ATT\&CK: e.g., Process Injection
Defense: System Call Analysis

Pseudocode:
remote_thread = search Thread:RemoteCreate
remote_thread = filter (start_function == "LoadLibraryA"
    or start_function == "LoadLibraryW")
remote_thread = filter (src_image_path != "C:\Path\To\
    TrustedProgram.exe")
output remote_thread

Logpoint SIEM:
norm_id=WindowsSysmon event_id=8 start_function IN ["
    LoadLibraryA", "LoadLibraryW"] -source_image="C:\Path\
    To\TrustedProgram.exe"
```

Listing 1.4. Sample from Cyber Analytics Repository

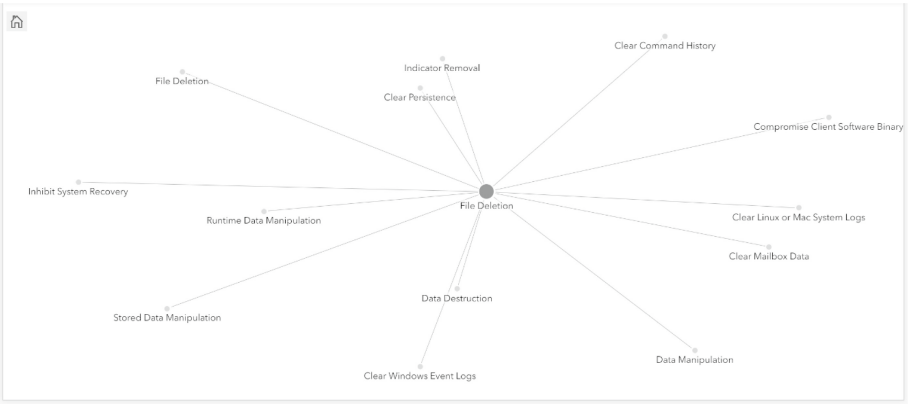

Fig. 8. Exploiting Data Components to detect Technique

6 Conclusion and Future Work

The risk of sensitive data being lost through data exfiltration is currently classified as high. In particular, the recent coupling with ransomware attacks increases the danger - keyword "multiple extortion". Our previous work shows that research has been devoted to this topic for many years. very good reviews of the numerous individual papers exist up to 2018. We have conducted a systematic literature search in a new forum "DTRAP" that is focused on practical solutions in the cyber security domain.

In doing so, we focused on the publications of the year 2022. It turned out that the work leading to these publications goes back to 2019. We pursue the goal of categorizing the data exfiltration methods studied last year. For this purpose, we evaluate three prominent methods for modeling and describing threats in cyberspace and specifically investigate the possibilities in the context of data exfiltration here. Based on the categorization, we now state results of our work:

There is a concentration of content, on the one hand, on technical countermeasures for data exfiltration at the IT network protocol level and, on the other hand, on automation in general for the risk of data exfiltration. We see here the need for further investigation of two of our categories. First, the category "Data Transfer Size Limit (T1030)[15]" and second, the category "Transfer Data to Cloud Account (T1537)[16]". We consider it very likely that techniques from these two categories will be used more frequently in the future. The amount of data which is processed in companies is rapidly increasing. So might the data volume, to be exfiltrated, have to increase. It will also be necessary for the attackers to split large amounts of data into smaller parts and then cleverly exfiltrate them in smaler sized parts. More and more companies are using cloud services. It will be easier for an attacker to hide the misuse of cloud services in the traces

[15] https://attack.mitre.org/techniques/T1030/.
[16] https://attack.mitre.org/techniques/T1537/.

of regular use of cloud services. In addition, cloud services scale and are suitable for discharging large amounts of data in total. The combination of techniques of both categories reveals disruptive damage potentials from the perspective of data exfiltration in the future. Our work helps to motivate further research at an early stage against the threat of this combination. However, the results of our systematic research show that no research focus has yet been formed in the community in this matter, at least not in this forum.

In view of the ISO 27001:2022 certification, it will be necessary to integrate threat intelligence into the basic processes of information security in the coming years. Our evaluation can be a starting point for further research to identify appropriate tools and services for this integration effort and to make pragmatic suggestions for companies that are now facing this task soon.

Suitable solutions against common threats of data exfiltration (e.g. Data Loss Prevention) are developed by software vendors. We see a need for further research here to determine whether it will be possible to detect and effectively combat even sophisticated methods of data exfiltration, such as the use of steganography. Steganography is utilized for covertly exfiltrating data. It is necessary to find out what methods can be used by attackers and what capacities are unleashed to leak the data as a result. For example, when using steganography, the amount of data that can be exfiltrated is certainly limited. But it is conceivable that passwords and crypto keys will first be extracted using steganographic techniques to prepare for the extraction of larger amounts of data.

In future work, we will take a deeper look at the process of data exfiltration. The entire attack-vector, at least the adjacent phases such as lateral movement of the attack-vector, potentially offer detection patterns to prevent the planned data exfiltration or to fully clarify it afterwards. This work could, in turn, uncover starting points to prevent the risk of data exfiltration in day-to-day operations.

References

1. Ahmed, M., et al.: MITRE ATT&CK-driven cyber risk assessment (2022). https://doi.org/10.1145/3538969.3544420
2. Alrehaili, M., Alshamrani, A., Eshmawi, A.: A hybrid deep learning approach for advanced persistent threat attack detection. In: The 5th International Conference on Future Networks & Distributed Systems, ICFNDS 2021, pp. 78–86. Association for Computing Machinery, New York (2022). ISBN: 9781450387347. https://doi.org/10.1145/3508072.3508085
3. Ayinala, S., Murimi, R.: On a territorial notion of a smart home. In: Proceedings of the 1st Workshop on Cybersecurity and Social Sciences, CySSS 2022, pp. 33–37. Association for Computing Machinery, New York (2022). ISBN: 9781450391771. https://doi.org/10.1145/3494108.3522766
4. Bhattarai, B., Huang, H.: SteinerLog: prize collecting the audit logs for threat hunting on enterprise network. In: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, ASIA CCS 2022, pp. 97–108. Association for Computing Machinery, New York (2022). ISBN: 9781450391405. https://doi.org/10.1145/3488932.3523261

5. Birnbach, S., Eberz, S., Martinovic, I.: Haunted house: physical smart home event verification in the presence of compromised sensors. ACM Trans. Internet Things **3**(3) (2022). ISSN: 2691-1914. https://doi.org/10.1145/3506859
6. Botacin, M., et al.: TERMINATOR: a secure coprocessor to accelerate real-time antiviruses using inspection breakpoints. ACM Trans. Priv. Secur. **25**(2) (2022). ISSN: 2471-2566. https://doi.org/10.1145/3494535
7. Carter, J., Mancoridis, S., Galinkin, E.: Fast, lightweight IoT anomaly detection using feature pruning and PCA. In: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, SAC 2022, pp. 133–138. Association for Computing Machinery, New York (2022). ISBN: 9781450387132. https://doi.org/10.1145/3477314.3508377
8. Chen, Z., et al.: Machine learning-enabled IoT security: open issues and challenges under advanced persistent threats. ACM Comput. Surv. **55**(5) (2022). ISSN: 0360-0300. https://doi.org/10.1145/3530812
9. Chignell, M., et al.: The evolution of HCI and human factors: integrating human and artificial intelligence. ACM Trans. Comput.-Hum. Interact. (2022). ISSN: 1073-0516. https://doi.org/10.1145/3557891
10. Clausen, H., Flood, R., Aspinall, D.: Traffic generation using containerization for machine learning. In: Proceedings of the 2019 Workshop on DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security, DYNAMICS 2019. Association for Computing Machinery, New York (2022). ISBN: 9781450384902. https://doi.org/10.1145/3464458.3464460
11. MISP Community. Malware Information Sharing Platform (MISP) User Guide: A Threat Sharing Platform (2022). https://www.circl.lu/doc/misp/book.pdf
12. MITRE Corporation. Cyber Threat Intelligence Repository Expressed in STIX 2.0 (2022). https://github.com/mitre/cti
13. MITRE Corporation. MITRE ATT&CK (2022). https://attack.mitre.org/
14. MITRE Corporation. MITRE ATT&CK Navigator: Web app that provides basic navigation and annotation of ATT&CK matrices (2022). https://github.com/mitre-attack/attack-navigator
15. MITRE Corporation et al.: Finding Cyber Threats with ATT&CK Based Analytics (2017). https://www.mitre.org/sites/default/files/2021-11/16-3713-finding-cyber-threats-with-attack-based-analytics.pdf
16. MITRE Corporation et al.: MITRE ATT&CK - Design and Philosophy (2020). https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
17. MITRE Corporation et al.: MITRE ATT&CK for Industrial Control Systems: Design and Philosophy (2020). https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf
18. Deochake, S., Channapattan, V.: Identity and access management framework for multi-tenant resources in hybrid cloud computing. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022. Association for Computing Machinery, New York (2022). ISBN: 9781450396707. https://doi.org/10.1145/3538969.3544896
19. European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Parliament, Brussel (2016)
20. ExtraHop. How to Monitor Sensitive Data & Stop Exfiltration via the Network (2022). https://www.extrahop.com/company/blog/2020/monitor-sensitive-data-and-stop-exfiltration-via-the-network/

21. Faulkenberry, A., et al.: View from above: exploring the malware ecosystem from the upper DNS hierarchy. In: Proceedings of the 38th Annual Computer Security Applications Conference, ACSAC 2022, pp. 240–250. Association for Computing Machinery, New York (2022). ISBN: 9781450397599. https://doi.org/10.1145/3564625.3564646
22. Giani, A., Berk, V.H., Cybenko, G.V.: Data exfiltration and covert channels (2006). https://www.spiedigitallibrary.org/conference-proceedings-of-spie/6201/620103/Data-exfiltration-and-covert-channels/10.1117/12.670123.short
23. Gorbett, M., Shirazi, H., Ray, I.: WiP: the intrinsic dimensionality of IoT networks. In: Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, SACMAT 2022, pp. 245–250. Association for Computing Machinery, New York (2022). ISBN: 9781450393577. https://doi.org/10.1145/3532105.3535038
24. de Gortari Briseno, J., Singh, A.D., Srivastava, M.: InkFiltration: using inkjet printers for acoustic data exfiltration from air-gapped networks. ACM Trans. Priv. Secur. **25**(2) (2022). ISSN: 2471-2566. https://doi.org/10.1145/3510583
25. Guan, Y., Li, Z., Xiong, G.: Research on novel TLS protocol network traffic management and monitoring method. In: Proceedings of the 7th International Conference on Cyber Security and Information Engineering, ICCSIE 2022, pp. 89–94. Association for Computing Machinery, New York (2022). ISBN: 9781450397414. https://doi.org/10.1145/3558819.3558835
26. Guarascio, M., et al.: Revealing MageCart-like threats in favicons via artificial intelligence. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022. Association for Computing Machinery, New York (2022). ISBN: 9781450396707. https://doi.org/10.1145/3538969.3544437
27. Hantke, F., Stock, B.: HTML violations and where to find them: a longitudinal analysis of specification violations in HTML. In: Proceedings of the 22nd ACM Internet Measurement Conference, IMC 2022, pp. 358–373. Association for Computing Machinery, New York (2022). ISBN: 9781450392594. https://doi.org/10.1145/3517745.3561437
28. Hernan, S., et al.: Uncover Security Design Flaws Using the STRIDE Approach (2019). https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach
29. Hittmeir, M., Mayer, R., Ekelhart, A.: Distance-based techniques for personal microbiome identification. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022. Association for Computing Machinery, New York (2022). ISBN: 9781450396707. https://doi.org/10.1145/3538969.3538985
30. Illumio. Zero Trust Segmentation delivers Cyber Resilience (2022). https://www.illumio.com/solutions/cyber-resilience
31. Inam, M.A., et al.: FAuSt: striking a bargain between forensic auditing's security and throughput. In: Proceedings of the 38th Annual Computer Security Applications Conference, ACSAC 2022, pp. 813–826. Association for Computing Machinery, New York (2022). ISBN: 9781450397599. https://doi.org/10.1145/3564625.3567990
32. MISP Standard - Collaborative Intelligence. Malware Information Sharing Platform (MISP) Program (2022). https://www.misp-project.org/
33. MISP Standard - Collaborative Intelligence. Python library using the MISP Rest API (2023). https://github.com/MISP/PyMISP
34. International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements (2022). https://www.iso.org/standard/82875.html

35. Joback, E., et al.: A statistical approach to detecting low-throughput exfiltration through the domain name system protocol. In: Proceedings of the 2020 Workshop on DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security, DYNAMICS 2020. Association for Computing Machinery, New York (2022). ISBN: 9781450387149. https://doi.org/10.1145/3477997.3478007
36. Kalderemidis, I., et al.: GTM: game theoretic methodology for optimal cybersecurity defending strategies and investments. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022. Association for Computing Machinery, New York (2022). ISBN: 9781450396707. https://doi.org/10.1145/3538969.3544431
37. Kapoor, M., et al.: Flurry: a fast framework for provenance graph generation for representation learning. In: Proceedings of the 31st ACM International Conference on Information & Knowledge Management, CIKM 2022, pp. 4887–4891. Association for Computing Machinery, New York (2022). ISBN: 9781450392365. https://doi.org/10.1145/3511808.3557200
38. Karagiannis, S., et al.: A-DEMO: ATT&CK documentation, emulation and mitigation operations: deploying and documenting realistic cyberattack scenarios - a rootkit case study. In: 25th Pan-Hellenic Conference on Informatics, PCI 2021, pp. 328–333. Association for Computing Machinery, New York (2022). ISBN: 9781450395557. https://doi.org/10.1145/3503823.3503884
39. Kumar, N., Handa, A., Shukla, S.K.: RBMon: real time system behavior monitoring tool. In: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, ASIA CCS 2022, pp. 1228–1230. Association for Computing Machinery, New York (2022). ISBN: 9781450391405. https://doi.org/10.1145/3488932.3527289
40. Ladisa, P., et al.: Towards the detection of malicious Java packages. In: Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses, SCORED 2022, pp. 63–72. Association for Computing Machinery, New York (2022). ISBN: 9781450398855. https://doi.org/10.1145/3560835.3564548
41. Lamshöft, K., Dittmann, J.: Covert channels in network time security. In: Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security, IH & MMSec 2022, pp. 69–79. Association for Computing Machinery, New York (2022). ISBN: 9781450393553. https://doi.org/10.1145/3531536.3532947
42. Landauer, M., et al.: A framework for automatic labeling of log datasets from model-driven testbeds for HIDS evaluation. In: Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Sat-CPS 2022, pp. 77–86. Association for Computing Machinery, New York (2022). ISBN: 9781450392297. https://doi.org/10.1145/3510547.3517924
43. Lang, M., et al.: The evolving menace of ransomware: a comparative analysis of pre-pandemic and mid-pandemic attacks. Digit. Threats (2022). ISSN: 2692-1626. https://doi.org/10.1145/3558006
44. Liu, Y., et al.: RAPID: real-time alert investigation with context-aware prioritization for efficient threat discovery. In: Proceedings of the 38th Annual Computer Security Applications Conference, ACSAC 2022, pp. 827–840. Association for Computing Machinery, New York (2022). ISBN: 9781450397599. https://doi.org/10.1145/3564625.3567997
45. Lyu, M., Gharakheili, H.H., Sivaraman, V.: A survey on DNS encryption: current development, malware misuse, and inference techniques. ACM Comput. Surv. **55**(8) (2022). ISSN: 0360-0300. https://doi.org/10.1145/3547331

46. Mahdavifar, S., et al.: Lightweight hybrid detection of data exfiltration using DNS based on machine learning. In: 2021 the 11th International Conference on Communication and Network Security, ICCNS 2021, pp. 80–86. Association for Computing Machinery, New York (2022). ISBN: 9781450386425. https://doi.org/10.1145/3507509.3507520
47. Mahmod, J., Hicks, M.: SRAM has no chill: exploiting power domain separation to steal on-chip secrets. In: Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2022, pp. 1043–1055. Association for Computing Machinery, New York (2022). ISBN: 9781450392051. https://doi.org/10.1145/3503222.3507710
48. Martins, C., Medeiros, I.: Generating quality threat intelligence leveraging OSINT and a cyber threat unified taxonomy. ACM Trans. Priv. Secur. **25**(3) (2022). ISSN: 2471-2566. https://doi.org/10.1145/3530977
49. Mundt, M., Baier, H.: Towards Mitigation of Data Exfiltration Techniques using the MITRE ATT&CK Framework (2022). https://www.unibw.de/digfor/publikationen/pdf/2021-12-icdf2c-mundt-baier.pdf
50. Microsoft. Microsoft Threat Modeling Tool (2022). https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
51. Microsoft. Microsoft Threat Modeling Tool threats (2022). https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
52. MITRE. MITRE ATT&CK framework (2021). https://attack.mitre.org/
53. Mohammed, A.S., et al.: Cybersecurity challenges in the offshore oil and gas industry: an industrial cyber-physical systems (ICPS) perspective. ACM Trans. Cyber-Phys. Syst. **6**(3) (2022). ISSN: 2378-962X. https://doi.org/10.1145/3548691
54. Moiz, A., Alalfi, M.H.: A survey of security vulnerabilities in Android automotive apps. In: Proceedings of the 3rd International Workshop on Engineering and Cybersecurity of Critical Systems, EnCyCriS 2022, pp. 17–24. Association for Computing Machinery, New York (2022). ISBN: 9781450392907. https://doi.org/10.1145/3524489.3527300
55. Moure-Garrido, M., Campo, C., Garcia-Rubio, C.: Detecting malicious use of DOH tunnels using statistical traffic analysis. In: Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, PE-WASUN 2022, pp. 25–32. Association for Computing Machinery, New York (2022). ISBN: 9781450394833. https://doi.org/10.1145/3551663.3558605
56. Mundt, M., Baier, H.: Threat-based simulation of data exfiltration towards mitigating multiple ransomware extortion. Digit. Threats Res. Pract. **23**, 1–23 (2022)
57. Mundt, M., Baier, H.: Threat-based simulation of data exfiltration towards mitigating multiple ransomware extortions. Digit. Threats (2022). ISSN: 2692-1626. https://doi.org/10.1145/3568993
58. Oz, H., et al.: A survey on ransomware: evolution, taxonomy, and defense solutions. ACM Comput. Surv. **54**(11s) (2022). ISSN: 0360-0300. https://doi.org/10.1145/3514229
59. Payne, B., Mienie, E.: Multiple-extortion ransomware: the case for active cyber threat intelligence. In: ECCWS 2021 20th European Conference on Cyber Warfare and Security, vol. 6, pp. 331–336 (2021)
60. Pöhn, D., Hommel, W.: TaxidMA: towards a taxonomy for attacks related to identities. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022. Association for Computing Machinery, New York (2022). ISBN: 9781450396707. https://doi.org/10.1145/3538969.3544430

61. Pradeep, A., et al.: A comparative analysis of certificate pinning in Android & iOS. In: Proceedings of the 22nd ACM Internet Measurement Conference, IMC 2022, pp. 605–618. Association for Computing Machinery, New York (2022). ISBN: 9781450392594. https://doi.org/10.1145/3517745.3561439
62. Sahu, I.K., Nene, M.J.: Model for IaaS Security Model: MISP Framework (2021). https://ieeexplore.ieee.org/abstract/document/9498375
63. Scandariato, R., Wuyts, K., Joosen, W.: A descriptive study of Microsoft's threat modeling technique (2013). https://link.springer.com/article/10.1007/s00766-013-0195-2
64. Shen, J., et al.: Gringotts: fast and accurate internal denial-of-wallet detection for serverless computing. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, pp. 2627–2641. Association for Computing Machinery, New York (2022). ISBN: 9781450394505. https://doi.org/10.1145/3548606.3560629
65. Shreeve, B., et al.: Making sense of the unknown: how managers make cyber security decisions. ACM Trans. Softw. Eng. Methodol. (2022). ISSN: 1049-331X. https://doi.org/10.1145/3548682
66. Stoleriu, R., Puncioiu, A., Bica, I.: Cyber attacks detection using open source ELK stack (2021). https://ieeexplore.ieee.org/abstract/document/9515120
67. Sun, Z., et al.: Recent advances in LoRa: a comprehensive survey. ACM Trans. Sen. Netw. **18**(4) (2022). ISSN: 1550-4859. https://doi.org/10.1145/3543856
68. Ullah, F., et al.: Data exfiltration: a review of external attack vectors and countermeasures. Univ. Bristol Bristol Res. **57**, 1–57 (2018)
69. Vaccari, I., et al.: Exploiting Internet of Things protocols for malicious data exfiltration activities (2021). https://ieeexplore.ieee.org/abstract/document/9493887
70. Vandeplas, C., Iklody, A.: Malware information sharing platform core software - open source threat intelligence and sharing platform (2022). https://github.com/MISP/MISP
71. Wala, F.B., Cotton, C.: "off-label" use of DNS. Digit. Threats **3**(3) (2022). ISSN: 2692-1626. https://doi.org/10.1145/3491261
72. Zeng, J., Zhang, C., Liang, Z.: Palantír: optimizing attack provenance with hardware-enhanced system observability. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, pp. 3135–3149. Association for Computing Machinery, New York (2022). ISBN: 9781450394505. https://doi.org/10.1145/3548606.3560570
73. Zeng, Z., Chung, C.-J., Xie, L.: Security challenges for modern data centers with IoT: a preliminary study. In: Companion Proceedings of the Web Conference 2022, WWW 2022, pp. 555–562. Association for Computing Machinery, New York (2022). ISBN: 9781450391306. https://doi.org/10.1145/3487553.3524857
74. Zipperle, M., et al.: Provenance-based intrusion detection systems: a survey. ACM Comput. Surv. **55**(7) (2022). ISSN: 0360-0300. https://doi.org/10.1145/3539605