ENABLING PROTECTION AGAINST DATA EXFILTRATION BY IMPLEMENTING ISO 27001:2022 UPDATE

Michael Mundt[1]and Harald Baier[2]

[1]Esri Deutschland GmbH, Bonn, Germany
[2]Bundeswehr University, Research Institute CODE, Munich, Germany

ABSTRACT

The risk of data theft has increased significantly over the past years. As a consequence, overwhelming damage is caused to institutions and private persons, respectively. Even the widespread ISO standard 27001 was updated recently in October 2022 to integrate data exfiltration aspects. Corresponding new security controls have been introduced. In this paper we review the ISO 27001:2022 with respect to data exfiltration and come up with recommendations on how recently integrated ISO 27001:2022 controls can be used in an operational environment. Based on that, we introduce and demonstrate the effectiveness of a proactive and dynamic concept by integrating a simulation cycle into the Information Security Management System (ISMS) and using cyber threat intelligence to provide us with information about current threats. We provide a prototype for the threat simulation cycle based on a smart combination of established and widely accepted cyber defence tools. Within our evaluation we show the feasibility of our targeted and dynamically configurable simulation of data exfiltration threats and thus support to thwart the actual cyber-attacks in advance. In all we contribute to prevent (or at least make it significantly more difficult) the threat of data exfiltration. Dynamic, threat aware and preventive cyber-defence is our objective, and we provide an updated concept which integrates conclusively into an ISO 27001:2022 compliant ISMS.

KEYWORDS

ISO 27001:2022 Update, Data Exfiltration, Control 5.7 Threat Intelligence, Threat Simulation

1. INTRODUCTION

With the aim of encountering new threats like the rising threat of data theft, the ISO 27001 standard, which is widely used, was updated in October 2022 and is now available in the ISO 27001:2022 version [1]. This also applies to the corresponding standard ISO 27002, which is now available in the version ISO 27002:2022 [2]. Both standards are essential sources for implementing an ISMS. Furthermore, ISO Standard 27001 is used for certification. Our work refers to the innovations and changes compared to the previous version. We show what innovations have been introduced to counter the enormous risk of data theft. All other recommendations that we review and make in the course of this work are based on the update of the ISO standard.

Based on these findings we show how the new ISO 27001:2022 Control 5.7 Threat Intelligence can be implemented. Strategical, tactical and operational layers of threat intelligence are considered. We examine what content can be used on all three levels to highlight the current threat of data theft by advanced attackers. Well-known methods and software applications such as Malware Information Sharing Platform (MISP) and the MITRE ATT&CK framework are

Dhinaharan Nagamalai (Eds): EMVL, EDUT, SECURA, AIIoT, CSSE -2023
pp. 43-59, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120505

included in these considerations. Higher-level concepts such as the STRIDE concept are also considered.

We are now aligning preventive measures based on the findings of the threat intelligence. Our work offers a proactive concept of how the most acute threats can now be simulated before such attacks happen. The focus is on countering the risk of data theft. With this goal we show how a data exfiltration threat simulation process can be implemented and integrated in an ISO-compliant, updated ISMS. Carefully selected security controls of the updated ISO standard are cleverly combined with each other. Protective measures against cyber threats are checked in a targeted and proactive manner. Identified attack vectors are broken down and sections of it are reproduced in the simulation. The techniques that prepare and execute adversarial data exfiltration are simulated to stimulate the existing technical protective measures. Digital traces left by the attack are recorded and classified as later-on training data using the key classifiers of the simulated attack. In this way, knowledge is gained about the effectiveness of one's own protective measures and time to improve them. The simulation forestalls the attack. The defender retains the initiative.

All parts of our work flow finally into a prototype demonstration. The simulation cycle is set up and operated. We use software frameworks that are available on the market. We use the framework Caldera to emulate the attack vector. The framework Velociraptor serves as the opponent for the digital-forensic securing of evidence data. The goal is a targeted, dynamic defence. The current threats and the risks to the company's relevant business assets are constantly being identified. The new control 5.7 threat intelligence is set to value. The threat of data exfiltration is our focus here. The simulation is configured to simulate this specific threat before it is applied by an attacker. In this way, existing protective measures are checked and optimised by skilfully gathering experience with the simulation. The simulation cycle is integrated into the ISO 27001 ISMS in a resource-saving manner.

2. RELATED WORK

We have evaluated the relevant literature on the various topics covered in this paper.

2.1. ISO 27001 update

There is now some work on the update. We look at some selected works as examples. Junaid first looks at the IS= 27001:2022 update in general terms and notes that the title has changed [3]. The new official title is "Information security, cybersecurity and privacy protection". The protection of privacy was added to the title. It is also noted that the use of cloud services has now been taken into account. It is once again stated that the new standard makes practical recommendations for controls in order to effectively implement and operate an ISMS. Our work is clearly different. By focusing on countering the threat of data exfiltration and implementing a concrete, new control, we clearly set ourselves apart from this work. Burgdorf and Jendrian also note changes. However, they focus on ISO 27002:2022, which offers more concrete details on the implementation of individual controls [4]. They also point out that the standard is supplemented thematically by industry-specific standards. ISO 27017, for example, is used for more specific risk assessment of cloud services and ISO 27701 for handling personal data. They also note that new categories of measures have been introduced: organisational, employee-related, physical and technical measures. In addition, they show the new hashtags that will be introduced to allow better filtering. On the one hand, they show how the control works for the respective risk: *#preventive*, *#detective*, *#corrective*. In addition, the security objective pursued is shown for each control: *#confidentiality*, *#integrity*, *#availability*. Finally, hashtags of the NIST Cyber Security Framework (NIST CSF) (website: https://www.nist.gov/cyberframework) are adopted to mark in

which phases the respective control has an impact: *#identify*, *#protect*, *#detect*, *#respond* and *#recover*. Our work uses security controls from all phases. The markers shown here help to filter and sift through the controls. The new controls are then shown separately, and the migration effort is made in favor of the update. Daniel, Sánchez-García, Mejía and Gilabert focus on risk assessment that incorporates analysis of threats and vulnerabilities [5]. They see security controls as an opportunity to mitigate existing risks. They evaluate the risk model proposed by ISO/IEC 27005:2022 [6]. They stress the importance of quantitative risk assessment and point out the importance of a continuous improvement process. Software tools available on the market for automated risk assessment are evaluated and compared. Our work differs significantly. We examine tools for the targeted implementation of the Control 5.7 Threat Intelligence and not the general risk assessment. Finally, let's look at Malatji's review [7]. He states that ISO 27002:2022 is more appropriate to provide guidelines on implementing the new security controls while ISO 27001:2022 is not describing formally specific security controls. It shows the basic division of the total of 93 security controls and also points out once again that cloud computing cyber security has now been included in the standard.

2.2. Simulation to counter the threat of data exfiltration

The European data protection board provides a first definition of data breach [8, pp.7-8]. The consequences of a loss of personal data are described. Required reactions are identified and documented. Examples for correct notifications in case of a data breach are given. However, no preventive measures are considered here. This clearly distinguishes the paper from our work. The risk of data loss is examined in a much more concrete way and also from the perspective of preventive measures in the paper [9]. Finally, we take up the results of these works [10][11]. Here our service consists in incorporating the updates of the ISO standards ISO/IEC 27001:2022 and ISO/IEC 27002:2022. This was not yet the case with these two works. Thus, the concept of preventive simulation of the greatest dangers of data loss is adopted and updated on the basis of the new framework conditions.

2.3. Tools supporting threat intelligence procedures

There are spare works that deal with threat intelligence tooling. The demand for the new control 5.7 Threat Intelligence is still too new for extensive evaluation having taken place. In our work, we investigate the suitability of methods that are widely used in use. We consider the Microsoft STRIDE model [12] as it may be utilised using the corresponding Microsoft Threat Modeling Tool [13]. We also use the MITRE ATT&CK framework [14] for our investigations. There is already some work on this, but its focus differs significantly from our work. Ahmed, Panda, Xenakis and Panaousis focus on cyber driven risk analysis for example [15]. Finally, we consider the MISP, which itself has already been studied in a few papers, f.e. for cyber defence detection [16] and IaaS security [17]. Instead of looking at these tools and frameworks individually, we examine how they can be used to implement the requirements of the new ISO standard for the Control 5.7 Threat Intelligence and make a recommendation.

3. IMPLEMENTING THREAT SIMULATION UNDERUPDATED CONDITIONS

We take up the concept of simulating a threat to data theft based on the current threat situation for sensitive data sets, collecting data that will later help protect defences. we pursue the goal of making protective measures dynamic, focusing on identified threats. In doing so, we take up the results of existing work [10] adapting the changed controls of the update of the standards. The result is our evaluation of how simulation can be integrated into a modernised ISO 27001:2022 certification in a resource-efficient manner.

3.1. Brief description of updates

The previous 114 controls in 14 sections have been reduced to 93 controls in four sections or categories. The newly introduced taxonomy makes a clear distinction between organisational, personnel, infrastructural (physical) and technical measures. No topics have been omitted. existing controls were reorganised and combined. New controls have been added. This update is to be implemented by 2025 as part of the certification or update.

3.2. Selection of longer existing Controls

In the previous work[12,pp.21-22], the controls from the older version of the ISO standard were used to describe the concept of the simulation cycle. In the first step, we now select the corresponding controls in the new taxonomy that correspond to the previous selection. The previously identified, leading actors[10,p.13] can be retained unchanged. Table 1 shows the Security Controls according to the updated taxonomy. Unchanged, the updated standard also indicates the need to improve the suitability, adequacy and effectiveness of the ISMS measures continually. Any case of nonconformity should be responded to by means of the cyclically recurring measures of continuous improvement described.

Table 1. Longer existing Security Controls implementing a simulation cycle [1, Annex A]

Nr	Name	Description
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented
5.12	Classification of information	Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adapted by the organisation
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release
5.34	Privacy and protection of personal identifiable information (PII)	The organisation shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed
8.33	Test information	Test information shall be appropriately selected, protected and managed

These steps correspond to those previously used[10, p.11] and it makes sense to integrate this cycle unchanged into the simulation process:

a) taking action to control and correct, b) deal with consequencesc) implement any action needed, d) review effectivenesse) make changes to ISMS if needed, f) document former nonconformity, action taken, g) document result of corrective action

3.3. Selection of new controls

The update of the standard brings new controls. Some of the new controls are perfectly suited to support process integration. To integrate the process for simulating current data theft threats, we also use the new controls shown in the list. The updated standard provides a brief description of each control in Appendix A[2, pp. 11-18]. Control 5.7 "Threat Intelligence" is used to collect and analyse information about threats to information security. Control 8.12 "Data leakage prevention"

points out that prevention measures against data leakage have to be applied to systems, networks and other devices that process, store or transmit sensitive information. Finally, the new control 8.16 "Monitoring activities" requires monitoring for anomalous behaviour as well as appropriate actions taken to evaluate potential information security incidents within networks,systemsand applications. A more detailed description of these controls can be found in ISO 27002:2022 [2]. For these new controls (Table 2), we evaluate the details in the following paragraphs.

Table 2. Further Security Controls to implement a simulation cycle [1, Annex A]

Nr	Name	Description
5.7	Threat Intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and other devices that process, store or transmit sensitive information
8.16	Monitoring activities	Networks,systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents

3.3.1. Control 5.7 Threat Intelligence

It is given the purpose to provide awareness of the organisation's threat environment so that the appropriate mitigation action can be taken[2, p. 15]. The objective implementing this control is to prevent the threat from causing harm or at least to reduce the impact. Three layers of threat intelligence should be considered as shown in Table 3. Processes should be implemented to include the gathered information into the ISMS of the organisation[2, p. 16]. Furthermore, the information shall be input to improve detective controls like firewalls and intrusion detection capabilities. Last not least, threat intelligence should feed test processes and techniques. Finally, organisations can receive and make use of threat intelligence produced by other sources.

Table 3. Three levels of threat intelligence

Nr	Name	Description
01	Strategic	Exchange of high-level information about the changing threat landscape (e.g., types of attackers or types of attacks)
02	Tactical	Information about attacker methodologies, tools and technologies involved
03	Operational	Details about specific attacks, including technical indicators

3.3.2. Control 8.12 Data leakage prevention

The purpose of this control is described as detection and prevention of unauthorised disclosure and extraction of information by individuals or systems[2, p. 100]. Prevention measures to system, networks and other devices that process, store or transmit sensitive information. This is definitely the control for which implementation our simulation will open up the possibility of continuous improvement. This control requires monitoring of channels of data leakage (e.g., email, file transfers, mobile devicesand portable storage devices) and acting to prevent information from leaking in the course of identifying, detecting and blocking the expose of sensitive information if it is not approved by an authorised authority. During implementation, a strong interaction with other controls of this standard can be observed.

3.3.3. Control 8.16 Monitoring activities

The purpose of this control is described as to detect anomalous behaviour and potential information security incidents [2, pp. 106-108]. The scope of monitoring should be adjusted in accordance with business requirements and comply with applicable regulations. The standard recommends including various data sources e.g., outbound and inbound network, system and application traffic, access to systems, servers, networking equipment, monitoring system, critical applications, etc., critical or admin level system and network configuration files, logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, event logs relating to system and network activity, use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance. Furthermore, diverse samples of anomalous behaviours to be detected are given. Tools for automated and continuous monitoring are required, ideal-wise monitoring takes place close to real-time. At the end some tips for implementation are given e.g., leveraging machine learning and artificial intelligence capabilities and using block-lists or allow-lists.

4. FINDINGS TO IMPLEMENT NEW CONTROL 5.7 THREAT INTELLIGENCE

In addition, we are evaluating different methods to implement the new Control 5.7 Threat Intelligence. First, the methods are briefly presented and evaluated.

4.1. Microsoft Threat Modelling 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 [18]. The underlying concept provides user functionality to design software architectures, which are then examined for threats in thecourse of the cyclic software development process. Identified threats are eliminated or suitably mitigated at the earliest possible stage in the software development cycle [19]. The threat analysis is based on the STRIDE model [20]. This categorises different types of threats: **S**poofing-**T**ampering-**R**epudiation-**I**nformation Disclosure-**D**enial of Service-**E**levation of Privilege. In our opinion, the tool is specifically suitable in the context of software development, but not for a comparatively more general implementation of the control. The categories of the STRIDE method, on the other hand, offer an excellent opportunity to summarize risk areas for companies and implement them in an aggregated form for corporate management.

4.2. MITRE ATT&CK

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[14, p. 21]. The framework consists of an entry web page [14] with interactive access to different matrices, a Cyber Threat Intelligence (CTI) repository [21] in Structured Threat Information eXpression (STIX) format, several companion documents[22][23][24], a python API [25], and an interactive application with basic functions for navigating, searching, tagging, and storing based on the information repository [26]. The framework provides a common taxonomy for structuring and describing Tactics, Techniques and Procedures (TTP). In our assessment 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.

4.3. MISP

This is an open-source threat intelligence and sharing platform. The MISP Core Software [27] facilitates exchange and sharing of threat information as well as Indicators of Compromise (IoC) about targeted malware and campaigns [28].

In our assessment, the purpose of the MISP software is the quick identification and modelling of current malware and its usage in current campaigns. MISP is also about sharing individual malware information in real-time. 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.

4.4. Strategical, tactical, operational threat intelligence

We examine the now required three layers of threat intelligence.

4.4.1. Strategical

The first recommended layer for implementing the threat intelligence control is the strategic one[2, p. 16]. It is described as handling high-level information about the changing threat landscape. From our point of view, this is a level that is ideally suited to preparing situation information for company management. It is important to reduce the technical complexity, to classify the overall threats of cyberspace in relation to relevant assets of the company and to compare them with the company's overriding security objectives, as defined in the ISMS security policy directed and guided by the company leadership. For this we recommend the STRIDE method. Detached from the software, we use this method specifically for the strategic evaluation in the course of the new Security Control[2, p. 15]. Our focus in this work is on the risk of data exfiltration.

Here, the category **I**nformation Disclosure of the STRIDE [20] method is suitable for explaining the current dangers that arise for the company due to the unwanted outflow of critical data to the company management in an overview.

4.4.2. Tactical

The ISO Standard provides additional guidance for mapping the tactical layer of threat intelligence[2, p. 16]. In our opinion, the required information about attacker methodologies, tools and technologies can be found most purposefully in the MITRE ATT&CK framework. The underlying data model offers information about APT and their attack vectors in a suitable way. This is validated information that was entered by experienced cyber analysts and is regularly curated by the MITRE organisation in terms of quality. The intentions (Tactics) of the known APTs are shown. It is possible to assess the way in which the threats affect the core processes of the business. Since the data model of the MITRE ATT&CK framework also includes the procedures and malware used by the APTs, an initial interaction with the management of technical vulnerabilities in Security Control 8.8 should be sought at this point. Looking at the opponent's data exfiltration, the interaction with the new control becomes visible. The protection of the critical assets (Security Control 5.33 Protection of records[2, pp. 53-54]) against adversarial data exfiltration is ideally based on currently expected attack vectors.

4.4.3. Operational

As far as the third layer is concerned, according to the ISO standard, it should be about specific attacks and technical indicators of Compromise (IoC). In addition, the demand is made that threat intelligence information is shared[2, pp. 16-17]. In the case of IoC, it makes sense to do the swapping near real-time. If possible, a concrete campaign should not affect any company or only one organisation and should not be able to spread unnoticed. This is where speed matters. Information is also shared in the MITRE ATT&CK framework. However, the character is rather curative. Quality is what counts here, not so much speed. In our opinion, the MISP is a good option for implementing the operational layer of threat intelligence. We recommend using MISP in order to establish networking with providers of threat intelligence and, if given, with other companies for the purpose of receiving or exchanging tactical information on malware currently in use and IoCs that have just become known. The functionality of labelling IoCs in the MISP with basic identifiers of the MITRE ATT&CK taxonomy is also particularly useful. With this functionality, the logical relationship between the operational and tactical layers can be directly integrated into the workflows. MISP offers therefore the construct of the galaxies and the MITRE ATT&CK galaxies are provided in machine readable format [29].

4.4.4. Short summary

Table 4 summarises our recommendation for implementing the new 5.7 Threat Intelligence control.

Table 4. Suggestion for implementing new Control 5.7 Threat Intelligence

Layer	Method	Format
Strategic	STRIDE	Document, on demand integration into ISMS document structure
Tactical	MITRE ATT&CK framework	Navigator, Custom Datapipeline [11, pp. 11-12], MISP Galaxies
Operational	MISP	MISP Feeds and data sources

Comparable solutions that implement the MITRE ATT&CK framework and at the same time allow the real-time exchange of IoC are currently emerging on the market, such as the Microsoft Sentinel product, which interacts with Microsoft Defender (Endpoint Detection).

5. IMPLEMENTING THE SIMULATION CYCLE

5.1. Concept

Mundt and Baier have identified foundational considerations for the implementation of threat simulation with the focus on the threat of data exfiltration [10][11]. We take these findings, adjust the reorganised and new ISO Security Controls for the concept and then implement the simulation prototypically. First, we start with the concept and describe it with a Business Process Modulation Notation (BPMN) diagram in Figure 1. We use a choreography diagram in order to show the interaction between participants and concentrate on the message flows and associations between the Security Controls. On the left side it starts with the inventory of the information. Knowing the assets is essential. The information is classified, labelled and then processed for business purposes. During processing an acceptable use is enforced.All business processing activities are logged. The processing is enabled by IT services. During business processing and therefore using IT services sensitive and personal identifiable information have to be protected.

Threat Intelligence is driving the monitoring of activities and the management of technical vulnerability. Threat intelligence helps to focus. Measures are taken for the IT services to prevent data leakage. Test information, based as closely as possible on the productive data in terms of shape, size and processing options, is provided. Depending on the results of threat analysis, the simulation is configured to target the most current threats and then run with the test information. Knowledge gained through the simulation is passed on to the continuous improvement cycle. The simulation is repeated cyclically. As a result, valuable input for risk assessment and for preventive and detective controls is risen. The simulation enriches security testing procedures.

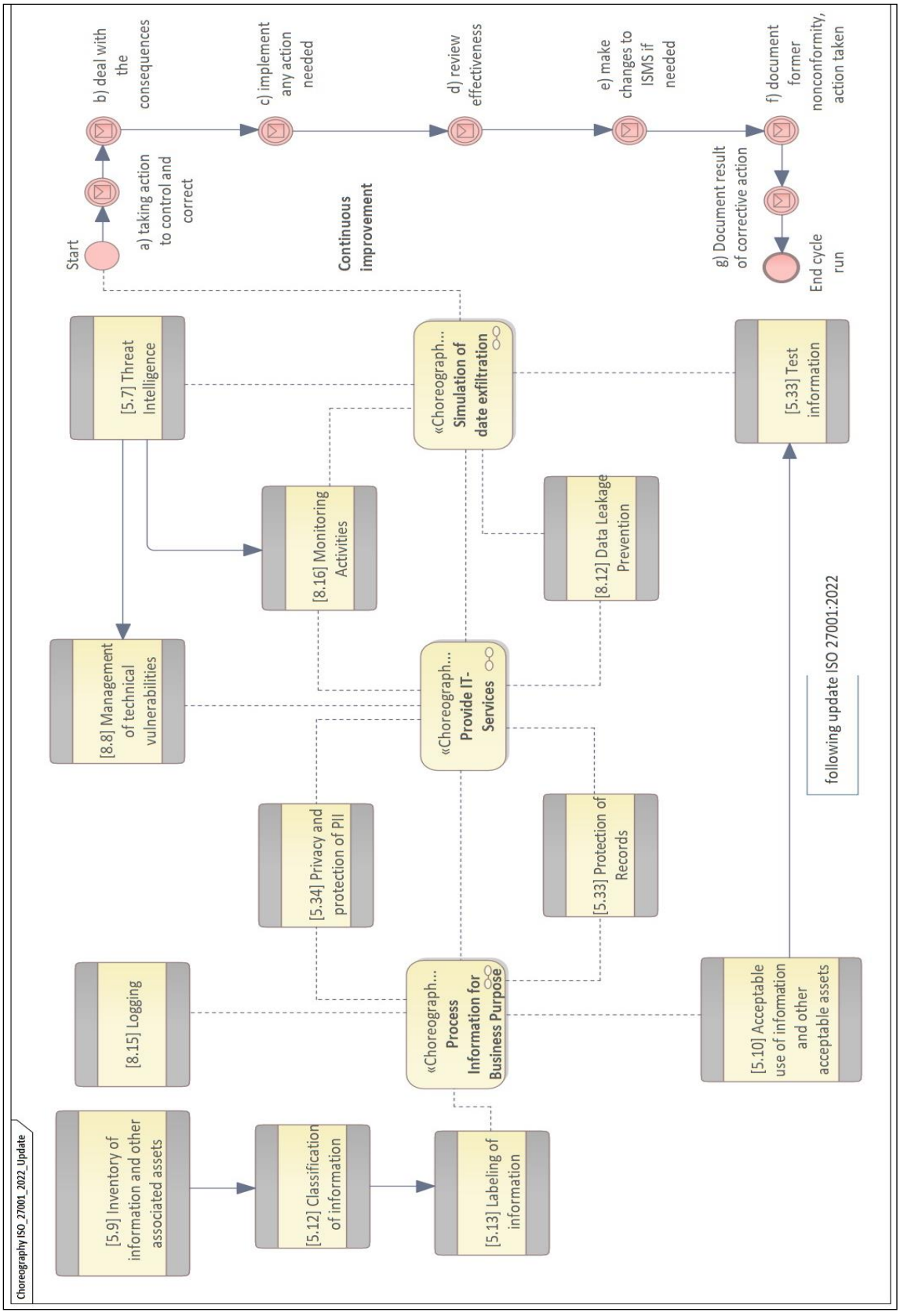

Figure 1. Integrating threat simulation into an updated ISMS

5.2. Prototyping

We use available frameworks. The Caldera framework (website: https://caldera.mitre.org) is used to simulate the attack vectors or selected parts of them. This framework conceptually maps the entire stock of Tactics of the MITRE ATT&CK framework. At the time of our work only the technical implementations of some Techniques are missing. Starting from a central administration, we deploy agents to the connected clients. The attack Techniques are later rolled out via these agents either to individual clients or simultaneously to all connected clients.Figure 2 shows the emulation of a so-called operation. Operations provide the functionality to configure and simulate attack vectors.

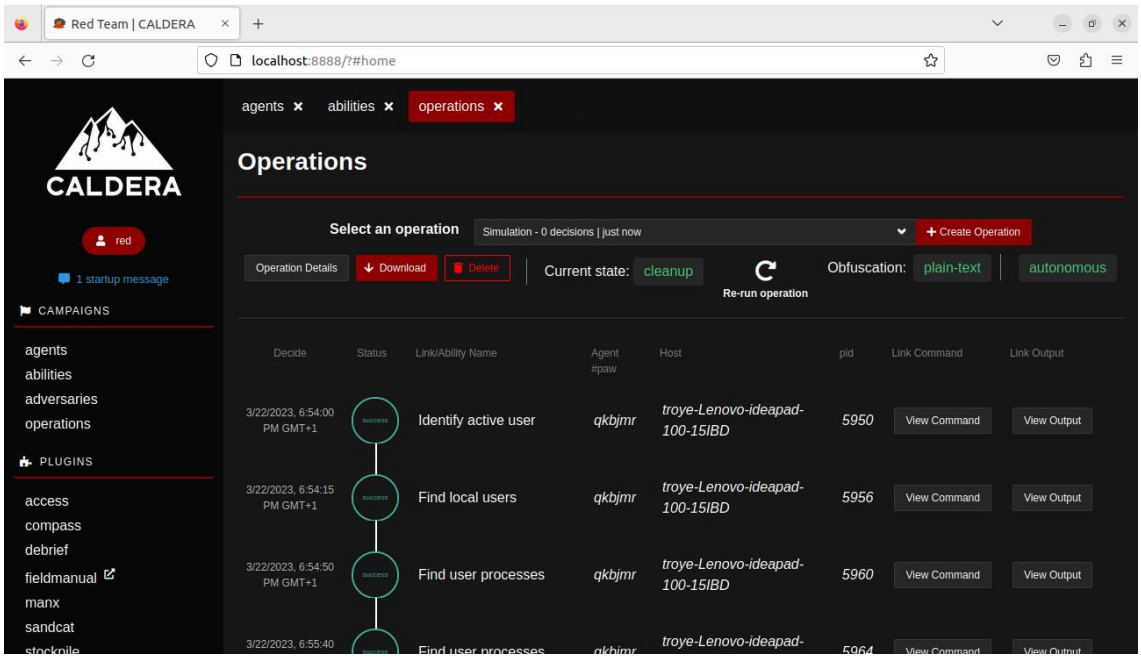

Figure 2. Simulating an attack vector with Caldera software framework

At the same time we roll out the Velociraptor (website: https://docs.velociraptor.app/) framework. Forensic associations to any data sources to be observed later on are developed and rolled out via the functionality of the framework. Figure 3 shows the roll out of a VQL statement to execute a YARA rule on the clients. VQL is the core capability of Velociraptor as a query language. Both frameworks interact with each other. We thus prove the feasibility of the concept as a prototype.

5.2. Samples

This concept is de facto already being applied proportionately. On GitHub there are collections of event logs that were collected on a windows client. A Technique is carried out here that is identified in the MITRE ATT&CK framework and then data is obtained from the windows event log.In this way, the connection between the triggering Technique and the receiving data source, in this case the Windows Event Logs, becomes visible and comprehensible [30]. Our simulation is also suitable for collecting this data and supplementing the GitHub repository.

The Caldera framework initiates the execution of the ATT&CK Technique and the Velociraptor framework grabs the Windows Event Logs. Both happen almost simultaneously, almost while the

technique is being performed. Listing 1 shows a VQL statement that is deployed via the Velociraptor framework and executed simultaneously on all connected clients of the system to be protected.The achievement of Mundt and Baier is to describe the process as a whole, instead of just looking at individual aspects, such as the Windows Event Log, detached from other sources [10].

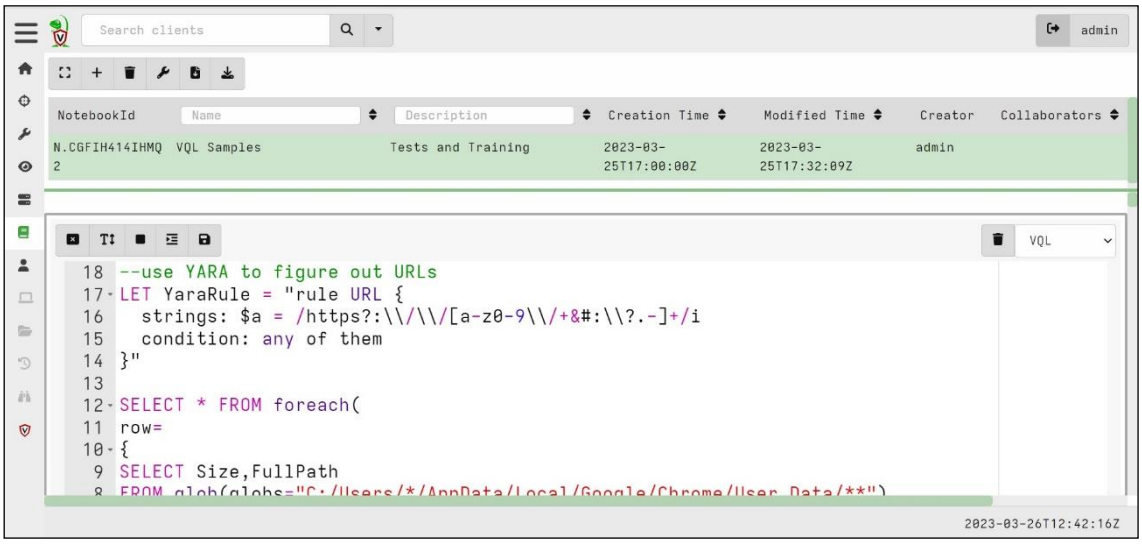

Figure 3. Collecting digital forensics evidence with Velociraptor software framework

Instead of a single Technique of the MITRE ATT&CK framework, we now simulate relevant parts of an attack vector. We consider the Tactics and their implementation with Techniques that contribute significantly to the preparation and implementation of data exfiltration.

Listing 1. Collecting Windows event logfiles

```
LET Files = SELECT * FROM glob(globs="C:/Windows/System32/winevt/Logs/*")
WHERE NOT IsDir AND FullPath =~ ".evtx$"
SELECT * FROM foreach(
 row={SELECT FullPath FROM Files},
 query={SELECT System.TimeCreated.SystemTime, System.Channel,
                    System.Execution.ProcessID, EventData.param3, Message FROM
                    parse_evtx(filename=FullPath)}
 )
```

For this prototypical proof, we configure the attack vector or parts of it manually. For this we use the navigator of the MITRE ATT&CK framework. We assume further on that in the course of the Cyber Threat Intelligence process it was determined that APT Sandworm Team is currently of particular threat importance. Using the ATT&CK Navigator, we select the group's known attack vector and mark the Techniques used in yellow. We look specifically at the Tactics (intermediate goals) that lead to data exfitration. We mark the techniques used here in orange. Figure 4 is showing an extract of this procedure. A higher degree of automation should certainly be sought

when the simulation is later implemented in a productive environment. The reading of the information from the MITRE ATT&CK framework as well as the extraction of relevant attack vectors or parts thereof as threats for relevant, sensitive information might then take place within the framework of a data pipeline. Here, manual configuration is certainly sufficient for this prototypical proof.

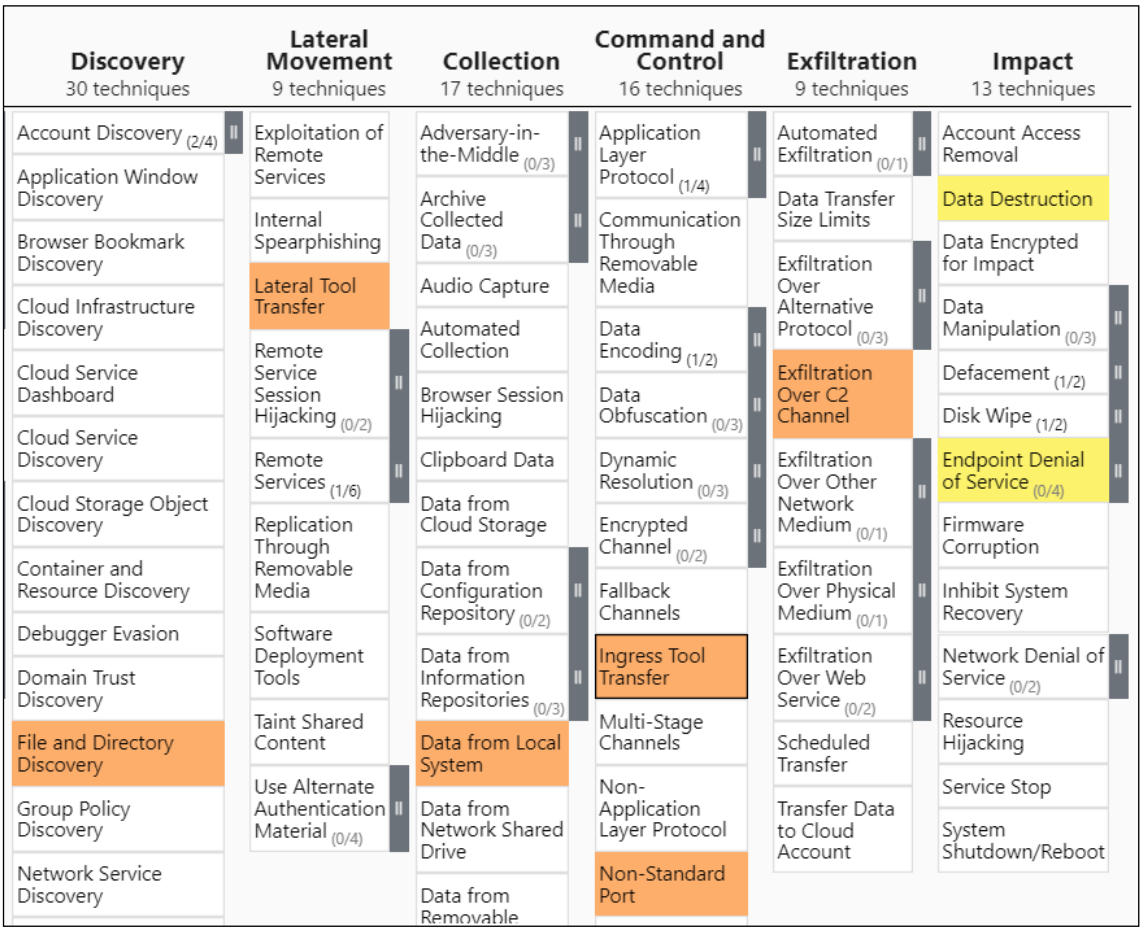

Figure 4. Extract of the enterprise IT attack Vector of APT Sandworm Team

We now configure the Techniques marked in orange as an Operation in the Caldera framework and thus prepare the simulation. Finally, we figure out the data sources that are corresponding to the Techniques in the simulation and implement a VQL script or artefact in order to hunt each Technique. We begin digital forensics hunting with Velociraptor. Then we start the simulation. All the incoming data during the hunt is carefully collected. The data combination of MITRE ATT&CK Technique and Velociraptor's data collection is stored in a structured manner and is henceforth available as training data.

This relationship is shown in the following tree structure. Furthermore, a VQL script is shown on a selected example how to monitor process creation in Listing 2. Many artifacts are already available through the community. This article [31] shows the query in VQL for the detection of a Cobalt Strike (website: https://www.cobaltstrike.com/) beacon. Cobalt Strike is very often used to implement the command-and-control infrastructure and thus is likely to be used by APT Sandworm to exfiltrate data.

[+] Tactic: Discovery
[+] Technique: File and DirectoryDiscovery(T1083), website: https://attack.mitre.org/techniques/T1083/
[+] Data Source: Command (DS0017), website: https://attack.mitre.org/datasources/DS0017/
[+] Data Component: Command Execution
[+] Data Source: Process(DS0009), website: https://attack.mitre.org/datasources/DS0009/
[+] Data Component: OS API Execution
[+] Data Component: **Process Creation**

The path is now being followed to monitor all data components continuously and to collect any data arising there. For this we use further VQL scripts and artifacts (website: https://docs.velociraptor.app/docs/gui/artifacts/) of the Velociraptor framework. We summarise more complex monitoring processes in hunting-objects which are then run for constantmonito-ring.

Listing 2. Monitoring process creation

```
SELECT * FROM MSFT_WmiProvider_ExecMethodAsyncEvent_Pre
        WHERE ObjectPath="Win32_Process" AND MethodName="Create"
```

6. CONCLUSION AND FUTURE WORK

Finally, the results of the work are summarised and we give an outlook.

6.1. Conclusion

The update of the standard ISO 27001:2022 offers new security controls. We use these new controls to procedurally integrate the simulation of current threats into the ISMS. Security Control 5.7 Threat Intelligence helps to tailor the simulation to existing attack vectors. Data is recorded during the simulation of the attack vector. Security Control 8.16 Monitoring activities & Networks helps to collect digital footprints that occur now. The configuration data of the simulation are merged with the collected data of the digital forensics in a structured way and are henceforth available as analysis and training data. The implementation of the simulation cycle was proven as a prototype.

6.2. Future Work

We continue our work on the simulation cycle. In the next step, we set up a collection of templates that help to capture the Techniques of the MITRE ATT&CK framework respectively the corresponding Data Components digitally forensically. We are emphatically pursuing the goal of building a counter-attack-vector simulation database that can help to put this simulation cycle into practice and to automate it in the medium term.

REFERENCES

[1] Cybersecurity ISO/IEC JTC 1/SC 27 Information security and Privacy Protection. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 2022. url: https:// www.iso.org/standard/82875.html (visited on 04/02/2023).

[2] Cybersecurity ISO/IEC JTC 1/SC 27 Information security and Privacy Protection. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. 2022. url: https://www.iso.org/standard/75652. html (visited on 04/04/2023).

[3] Ta-Seen Junaid. ISO 27001: Information Security Management Systems. 2023. url: https : / / www . researchgate . net / profile / Ta - Seen - Junaid / publication / 367166657_ISO_27001 (visited on 04/03/2023).

[4] Milan Burgdorf and Kai Jendrian. ISO 27002 revisited. 2022. url: https://link. springer.com/article/10.1007/s11623-022-1607-6 (visited on 04/03/2023).

[5] Isaac Daniel et al. Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. 2023. url: https://www.mdpi.com/2076-3417/13/1/395 (visited on 04/03/2023).

[6] Cybersecurity ISO/IEC JTC 1/SC 27 Information security and Privacy Protection. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. 2022. url: https://www.iso.org/standard/80585. html (visited on 04/11/2023).

[7] 2023 International Conference On Cyber Management MalatjiMasike, Engineering (CyMaEn) Cyber Management, and Engineering (CyMaEn). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. 2023. url: https : //ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10051114 (visited on 04/03/2023).

[8] Europen Data Protection Board (edpb). Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0. 2023. url: https : / / edpb . europa .eu / system / files / 2023 - 04 / edpb _ guidelines _ 202209 _ personal _ data _ breach _ notification_v2.0_en.pdf (visited on 04/03/2023).

[9] Ivan Vaccari et al. Exploiting Internet of Things Protocols for Malicious Data Exfiltration Activities. 2021. url: https://ieeexplore.ieee.org/abstract/document/ 9493887.

[10] Michael Mundt, Harald Baier. Towards Mitigation of Data Exfiltration Techniques using the MITRE ATT&CK Framework. 2022. url: https : / / www . unibw . de / digfor/publikationen/pdf/2021-12-icdf2c-mundt-baier.pdf.

[11] Michael Mundt and Harald Baier. “Threat-Based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions”. In: Digital Threats (Nov. 2022). Just Accepted. issn: 2692-1626. doi: 10.1145/3568993. url: https://doi. org/10.1145/3568993.

[12] Microsoft Corporation. STRIDE-Model. 2023. url: https://learn.microsoft. com / en - us / azure / security / develop / threat - modeling - tool - threats # stride-model (visited on 04/10/2023).

[13] Riccardo Scandariato, Kim Wuyts, and WouterJoosen. A descriptive study of Microsoft’s threat modeling technique. 2013. url: https : / / link . springer . com / article/10.1007/s00766-013-0195-2.

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

[15] Mohamed Ahmed et al. MITRE ATT&CK-driven Cyber Risk Assessment. 2022. url: https://dl.acm.org/doi/abs/10.1145/3538969.3544420.

[16] R˘azvanStoleriu, Alin Puncioiu, and Ion Bica. Cyber Attacks Detection Using Open Source ELK Stack. 2021. url: https://ieeexplore.ieee.org/abstract/document/ 9515120.

[17] Indra Kumar Sahu and Manisha J Nene. Model for IaaS Security Model: MISP Framework. 2021. url: https : / / ieeexplore . ieee . org / abstract / document / 9498375.

[18] Microsoft. Microsoft Threat Modeling Tool. 2022. url: https://learn.microsoft. com/en-us/azure/security/develop/threat-modeling-tool.

[19] Shawn Hernan et al. Uncover Security Design Flaws Using The STRIDE Approach. 2019. url: https://learn.microsoft.com/en- us/archive/msdn- magazine/ 2006/november/uncover-security-design-flaws-using-the-stride-approach.

[20] Microsoft. Microsoft Threat Modeling Tool threats. 2022. url: https : / / learn . microsoft . com / en - us / azure / security / develop / threat - modeling - tool - threats.

[21] MITRE Corporation. Cyber Threat Intelligence Repository expressed in STIX 2.0. 2022. url:https://github.com/mitre/cti.

[22] MITRE Corporation et al. MITRE ATT&CK - Design and Philosophy. 2020. url: https : / / attack mitre . org / docs / ATTACK _ Design _ and _ Philosophy _ March _ 2020.pdf.

[23] MITRE Corporation et al. MITRE ATT&CK for Industrial Control Systems: Design and Philosophy. 2020. url: https://attack.mitre.org/docs/ATTACK_for_ICS_ Philosophy_March_2020.pdf.
[24] MITRE Corporation et al. Finding Cyber Threats with ATT&CK based Analytics. 2017. url: https://www.mitre.org/sites/default/files/2021-11/16-3713- finding-cyber-threats-with-attack-based-analytics.pdf.
[25] MITRE Corporation. mitreattack-python. 2022. url: https://github.com/mitreattack/mitreattack-python.
[26] MITRE Corporation. MITRE ATT&CK Navigator: Web app that provides basic navigation and annotation of ATT&CK matrices. 2022. url: https : / / github . com/mitre-attack/attack-navigator.
[27] Christophe Vandeplas and Andras Iklody. Malware Information Sharing Platform core software - Open Source Threat Intelligence and Sharing Platform. 2022. url: https://github.com/MISP/MISP.
[28] MISP Community. Malware Information Sharing Platform (MISP) User Guide: A Threat Sharing Platform. 2022. url: https://www.circl.lu/doc/misp/book.pdf.
[29] Christophe Vandeplas et al. Github: misp-galaxies. 2023. url: https://github. com/MISP/misp-galaxy/blob/main/clusters/mitre-attack-pattern.json.
[30] gwsalessbousseadengwsales. EVTX-ATTACK-SAMPLES, Windows EVTX Samples. 2021. url: https : / / github . com / sbousseaden / EVTX - ATTACK - SAMPLES / blob/master/README.md (visited on 04/12/2023).
[31] Mike Cohen. Cobalt Strike Payload Discovery And Data Manipulation In VQL. 2021. url: https://velociraptor.velocidex.com/cobalt- strike- payloaddiscovery-and-data-manipulation-in-vql-4310349e67c (visited on 04/12/2023).

AUTHORS

Michael Mundt has been employed atthecompany Esri Deutschland GmbH since 2003. The collaboration with Professor Baier began in April 2021. He received his university diploma as asurveyor in 1997 and completed his second degree, Master Engineer, in IT security and digital forensics in 2020.

PROF. DR. Harald Baier received his doctorate in 2002 from the TU Darmstadt for a thesis on efficient generation of elliptic curves. He was an employee since 2020 at the research institute CODE of the Faculty of Computer Science at the University of the Bundeswehr Munich. There he is a professor digital forensics. His work therefore focuses on different aspects of digital forensics.